A SYSTEMIC PERSPECTIVE FOR U.S. OPEN BANKING: ENSURING PARTICIPATION, ACCESS, AND STABILITY

Scott Farrell[*]

Abstract

Finally, open banking is on a path to be established in the United States after more than a decade since the laying of its legislative foundation in the Dodd-Frank Act. With the issuance of an advance notice of proposed rulemaking by the Consumer Financial Protection Bureau, and the Executive Order on Promoting Competition in the American Economy, regulatory momentum is building. However, there is much work to be done in the legal design of rights, responsibilities, and relationships under open banking in the U.S. before it can empower consumers to derive value from their banking data. Fundamental issues need to be addressed including what data is covered, in what form it is provided, how the holding and use of the information is controlled, the security and accuracy of the shared data, and the transparency of the data sharing. A broader perspective of open banking as a system will also be necessary to ensure the participation of banks, data recipients, intermediaries and other service providers needed to deliver wider economic outcomes relating to competition, innovation, inclusion, and consumer protection. This Article explains a systemic perspective of open banking as a network of interconnected and interdependent participants sharing valuable customer data and analyses how access and stability need to be balanced in open banking's legal design. It compares the legal features which manage participation in the established open banking systems of Australia and the United Kingdom and evaluates them against equivalent legal features in banking payment systems, which are also networks for the communication of valuable information. Through this comparison and evaluation, this Article finds that the United Kingdom (U.K.) open banking offers a lower level of regulation of indirect participation and outsourcing than Australian open banking and more limited rights to suspend participation and less clear protection of the value in customer data in participant default and insolvency. It also shows that the design of access and stability under Australian open banking is more aligned with banking payment systems in the management of potentially systemic risks. By demonstrating how differing legal

---

* Adjunct Professor, School of Private and Commercial Law, UNSW Sydney, and Partner, King & Wood Mallesons. I would like to thank Scientia Professor Ross Buckley, Professor Douglas Arner, and Dr. Anton Didenko for their ideas and guidance, the Australian Research Council Laureate Fellowship (FL200100007) for its financial support of this research, and Jack Zhou for their most helpful research assistance. The views expressed herein are mine, and not necessarily those of the Australian government, the Australian Research Council, King & Wood Mallesons or those who have assisted me with this research.

approaches to balancing access and stability in open banking can affect the participation on which open banking's success depends, this analysis will be critical for the design of America's open banking system.

INTRODUCTION 3

I. OPEN BANKING SYSTEMS 6
A. *Functions of Open Banking* 6
1. Data Portability 7
2. Customer Autonomy 9
3. Recipient Accountability 10
B. *Objectives of Open Banking* 10
1. Improving Competition 11
2. Encouraging Innovation 13
3. Fostering Inclusion 14
4. Consumer Protection 15
C. *Foundations of Participation in Open Banking Systems* 17
1. Enabling Access to Participation in Open Banking Systems 17
2. Preserving Stability of Participation in Open Banking Systems 19
D. *Summary* 22

II. FUNCTIONAL EQUIVALENCE WITH BANKING PAYMENT SYSTEMS 22
A. *Functional Equivalence from a Customer Perspective* 22
B. *Functional Equivalence from a Systemic Perspective* 24
1. Enabling Access to Participation in Banking Payment Systems 24
2. Stability 25
C. *Summary* 27

III. RELEVANCE OF OPEN BANKING IN AUSTRALIA AND THE U.K. TO THE U.S. 28
A. *The Legal Foundation for Open Banking in Australia* 29
1. The Legal Foundation for Open Banking in the U.K. 29

IV. ENABLING ACCESS TO PARTICIPATION IN OPEN BANKING SYSTEMS....31
A. *Direct Participation*....32
1. Comparison of Authorization to be a Data Recipient in Open Banking....32
2. Evaluation Against Conditions to Access Payment Systems....35
B. *Indirect Participation*....37
1. Comparison of Indirect Participation in Open Banking....37
2. Evaluation Against Indirect Participation in Payment Systems....42
C. *Outsourcing Arrangements*....43
1. Comparison of Regulation of Outsourcing Arrangements in Open Banking....43
2. Evaluation Against Regulation of Outsourcing in Payment Systems....45
D. *Summary*....48

V. PRESERVING STABILITY OF PARTICIPATION IN OPEN BANKING SYSTEMS....49
A. *Removal of Defaulting Participants*....49
1. Comparison of Removal of Defaulting Participant in Open Banking....49
2. Evaluation Against Removal of Defaulting Participant from Payment Systems....52
B. *Protecting Customer Value on Participant Default*....53
1. Comparison of Protection of Customer Data in Open Banking....53
2. Evaluation Against Protection of Customer Value in Payment Systems....55
C. *Managing Participant Insolvency*....56
1. Comparison of Management of Participant Insolvency in Open Banking....56
2. Evaluation Against Insolvency Law Protection for Payment Systems....59
D. *Summary*....60

VI. LESSONS FOR PARTICIPATION, ACCESS AND STABILITY IN U.S. OPEN BANKING....60

INTRODUCTION

After more than a decade since the laying of open banking's legislative foundation with the passing of section 1033 of the Dodd-Frank

Act in 2010 (Dodd-Frank Act),[1] regulatory momentum is now building for its implementation in the United States. With the issuance of an advance notice of proposed rulemaking (ANPR) by the Consumer Financial Protection Bureau (CFPB) in 2020,[2] and the Executive Order on Promoting Competition in the American Economy in mid-2021,[3] there is a clear regulatory intention for open banking in the U.S. to progress. With the aims to "facilitate the portability of consumer financial transaction data so consumers can more easily switch financial institutions and use new, innovative financial products,"[4] and harness technology to "give American families the power to more easily fire poor-performing banks,"[5] there is little time to lose.

However, there are many issues to consider and much work to be done in the legal design of rights, responsibilities, and relationships under U.S. open banking.[6] Although the Dodd-Frank Act provides a legislative foundation for information on a consumer's financial product or service to be made available to a consumer,[7] critical detail is to be set out in rules of the CFPB and the standards which are to apply. These need to cover fundamental issues including how access is to be provided, what data is covered, in what form it is provided, how the holding and use of the information is controlled, the security and accuracy of the shared data, and the transparency of the data sharing.[8] Submissions to the CFPB show that these are complicated matters with competing interests and views.[9]

---

1. Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010 § 1033, 12 U.S.C. § 5533 (hereinafter Dodd-Frank Act).

2. Bureau of Consumer Fin. Prot., Consumer Access to Financial Records, 85 Fed. Reg. 71,003 (proposed Nov. 6, 2020).

3. Exec. Order No. 14,036 on Promoting Competition in the American Economy, 86 Fed. Reg. 36,987 (July 9, 2021).

4. *Id*.

5. CONSUMER FIN. PROT. BUREAU, *Prepared Remarks of CFPB Director Rohit Chopra on the Overdraft Press Call* (Dec. 1, 2021), https://www.consumerfinance.gov/about-us/newsroom/prepared-remarks-cfpb-director-rohit-chopra-overdraft-press-call/ [https://perma.cc/5MX8-JD5J].

6. Bureau of Consumer Fin. Prot., Consumer Access to Financial Records, 85 Fed. Reg. 71,003 (proposed Nov. 6, 2020). *See* CHERYL R. COOPER, CONG. RSCH. SERV., IN11745, OPEN BANKING, DATA SHARING, AND THE CFPB'S 1033 RULEMAKING (2021).

7. Dodd-Frank Act § 1033, 12 U.S.C. § 5533 (2010) ("Subject to the rules prescribed by the Bureau, a covered person shall make available to a consumer, upon request, information in the control or possession of the covered person concerning the consumer financial product or service that the consumer obtained from such covered person.").

8. *See* CONSUMER FIN. PROT. BUREAU, CONSUMER PROTECTION PRINCIPLES: CONSUMER-AUTHORIZED DATA SHARING AND AGGREGATION (Oct. 18, 2017), https://files.consumerfinance.gov/f/documents/cfpb_consumer-protection-principles_data-aggregation.pdf [https://perma.cc/VAH2-56XX].

9. *See* CONSUMER FINANCIAL PROTECTION BUREAU, CFPB SYMPOSIUM: CONSUMER ACCESS TO FINANCIAL RECORDS (Feb. 26, 2020), https://www.consumerfinance.gov/about-us/events/archive-past-events/cfpb-symposium-consumer-access-financial-records/ [https://perma.

Fortunately, America is not alone in its open banking journey. Open banking is an "evolving trend in many jurisdictions,"[10] and valuable insights can be drawn from the experiences in developing the legal framework for open banking elsewhere, including Australia and the U.K. which are the leading common law jurisdictions in establishing regulated open banking frameworks.[11] One of these insights is the need to design open banking holistically as a system and not solely as a technological framework to enable data transfers by consumers. This is because the broader objectives of open banking, such as encouraging competition, enabling innovation, improving inclusion and consumer protection,[12] require the participation not only of customers and banks but also recipients who use customer data to enable better choices and more convenience for customers and the service providers that support them. To achieve these goals, open banking needs to be designed to provide access to these participants and preserve the stability of the system for the sharing of customer data which emerges.

This Article argues that this broader perspective requires systemic analysis of open banking by reference to the fundamental issues of participation, access and stability in banking payment systems. It demonstrates how this systemic perspective of open banking can be adopted by analyzing the legal features which govern participation in open banking in Australia and the U.K. and evaluating them against equivalent legal features which are designed to balance the provision of fair access and preservation of stability in banking payment systems. In conducting this analysis and evaluation, this Article shows how the legal design of U.K. open banking compensates for more limited flexibility in access by direct participation, more flexibility in access, and indirect participation, which results in a lower level of regulation of indirect participation and outsourcing relationships than under Australian open banking. It has identified that the legal design of U.K. open banking offers less in the preservation of stability due to more limited rights to suspend participation and less clear protection of the value in customer data in participant default and insolvency. It further shows that Australian open banking is more aligned with the legal features which provide

---

cc/MCZ3-9FMC]. *See also* the comment letters on the ANPR: REGULATIONS.GOV, Comments to *Consumer Access to Financial Records* (Nov. 6, 2020), https://www.regulations.gov/document/CFPB-2020-0034-0001/comment [https://perma.cc/DU75-KPX4] (last visited July 18, 2021).

10. BANK FOR INT'L SETTLEMENTS, REPORT ON OPEN BANKING AND APPLICATION PROGRAMMING INTERFACES 4 (2019) (these jurisdictions include Australia, Brazil, Canada, the European Union, Hong Kong, India, Israel, Japan, Malaysia, Mexico, New Zealand, Nigeria, Russia, Singapore, South Korea and the United Kingdom). *See* COMPETITION & MKTS. AUTH., *Update on Open Banking* (Nov. 5, 2021), https://www.gov.U.K./government/publications/update-governance-of-open-banking/update-on-open-banking [https://perma.cc/JM62-B7G6].

11. *See infra* section III.

12. *See infra* section I.A.2.

access and protect stability in those payment systems than U.K. open banking. Counter-intuitively, this is largely because U.K. open banking is established as part of the regulation of payments, whilst Australian open banking is established as the first part of a new and independent economy-wide consumer data right.

These conclusions should be valuable in the design of open banking in the U.S., particularly in relation to the need to take a systemic perspective in open banking's design. This Article demonstrates how ignoring this perspective in designing open banking can lead to the emergence of inefficiencies and systemic risks which can obstruct the achievement of open banking's goals.

Part I of this Article introduces the functions and objectives of open banking and the foundations of participation. Part II describes how those functions and foundations which relate to customer data are equivalent to those in banking payment systems which relate to customer funds. The legal structure of the open banking systems of Australia and the U.K. are introduced in Part III and their relevance explained. Part IV analyses the legal features which enable *access* to participation in Australian and U.K. open banking through direct and indirect participation and outsourcing arrangements and evaluates them against the legal features performing equivalent functions in banking payment systems. Part V analyses the legal features which preserve *stability* of participation in open banking through the management of participant default, the protection of customer value and the management of insolvency under Australian and U.K. open banking and evaluates them against the legal features performing equivalent functions in banking payment systems. Part 6 identifies and analyses the lessons from the analysis for balancing access and stability in participation in the legal design of America's open banking system.

I. OPEN BANKING SYSTEMS

A. *Functions of Open Banking*

Despite its adoption across many different jurisdictions globally, open banking has no widely accepted legal definition.[13] One is not attempted

13. *See*, *e.g.*, NYDIA REMOLINA, OPEN BANKING: REGULATORY CHALLENGES FOR A NEW FORM OF FINANCIAL INTERMEDIATION IN A DATA-DRIVEN WORLD (SMU Ctr. for AI & Data Governance) (2019); Christopher C. Nicholls, *Open Banking and the Rise of FinTech: Innovative Finance and Functional Regulation*, 35 BANKING & FIN. L. REV. 121, 122 (2019); Alessandro Palmieri & Blerina Nazeraj, *Open Banking and Competition: An Intricate Relationship*, 6 EU AND COMPAR. L. ISSUES & CHALLENGES SERIES (ECLIC) 217, 218 (2021); Ross P. Buckley et al., *Australia's Data-Sharing Regime: Six Lessons for the World*, KING'S L.J. (forthcoming); Daniel Gozman, Jonas Hedman & Kasper Sylvest Olsen, *Open Banking: Emergent Roles, Risks & Opportuniti*es 19 (AIS Research Papers No. 183, 2018); Linda Jeng, *Inception to Open Banking*, *in* OPEN BANKING 1 (Linda Jeng ed., 2022).

in the Dodd-Frank Act,[14] and it is not defined in the legislative instruments which establish and govern open banking in the U.K. and Australia,[15] the legislative instrument of its foundation in the European Union (EU),[16] or the documents which form its foundation in Hong Kong,[17] or Singapore.[18] Instead, it is more common for open banking's purpose, or the functions it performs, to be described than for its meaning to be defined. For example, the Congressional Research Service describes open banking as "the practice of giving financial services firms access to customer banking and other financial data to facilitate the development of new types of products and services for consumers."[19] The Bank for International Settlements (BIS) describes open banking as: "the sharing and leveraging of customer-permissioned data by banks with third party developers and firms to build applications and services, such as those that provide real-time payments, greater financial transparency options for account holders, and marketing and cross-selling opportunities."[20] These descriptions, and others suggested by scholars,[21] emphasize three functions of open banking from the perspective of the bank's customer: (1) data portability; (2) customer autonomy; and (3) recipient accountability.

1. Data Portability

Open banking is a form of data portability in that it enables customer banking data to be shared.[22] However, unlike the data portability rights

14. Dodd-Frank Act § 1033, 12 U.S.C. § 5533 (2010). This is understandable since the phrase "open banking" was not in common use at that time.

15. *See infra* section III.

16. Directive 2015/2366/EU, of the European Parliament and of the Council of Nov. 25, 2015 on Payment Services in the Internal Market, amending Directives 2002/65/EC, 2009/110/EC, and 2013/36/EU and Regulation (EU) No 1093/2010 and repealing Directive 2007/64/EC, 2015 O.J. (L 337) 35.

17. Hong Kong Monetary Auth., *Open API Framework for the Hong Kong Banking Sector* ,https://www.hkma.gov.hk/media/eng/doc/key-information/press-release/2018/20180718e5a2.pdf [https://perma.cc/8WG9-LYZV] (last vistied July 21, 2018).

18. ASS'N OF BANKING IN SING. & MONETARY AUTH. OF SING., ABS-MAS FINANCIAL WORLD: FINANCE-AS-A-SERVICE API PLAYBOOK (2016).

19. COOPER, *supra* note 6 at 1.

20. BANK FOR INT'L SETTLEMENTS, *supra* note 10, at 4 n. 1.

21. *See, e.g.*, Ana Badour & Domenic Presta, *Open Banking: Canadian and International Developments*, 34 BANKING & FIN. L. REV. 41, 42 (2018). *See also* Fernando Zunzunegui, *Digitalisation of Payment Services* 8 (Ibero-Am. Inst. for Law & Fin., Working Paper No. 1/2018, 2018); Nicholls, *supra* note 13; Jeng, *supra* note 13.

22. *See* Inge Graef, et al., *Spill-Overs in Data Governance: The Relationship Between the GDPR's Right to Data Portability and EU Sector-Specific Data Access Regimes* (Tilburg L. & Econ. Ctr., Tilburg Univ., Discussion Paper No. DP 2019-005, April 2019) (finding that it might also be described as a form of data access, but the distinction is not relevant here). *But see* Paul De Hert, et al., *The Right to Data Portability in the GDPR: Towards User-Centric Interoperability of Digital Services*, 34 COMPUT. L. & SEC. REV. 193 (2018).

provided under the EU's General Data Protection Regulation (GDPR),[23] open banking requires that data be shared in a standardized form,[24] which is interoperable between technology systems (syntactic portability) and meaningful to the recipient (semantic interoperability).[25] These requirements are critical to achieving the objectives of open banking, as the information derived from the customer data must be receivable and understandable by the recipient with whom the customer has chosen to share their data.[26]

Data portability in open banking is supported by the use of interoperable, standardized data technology, primarily Application Programming Interfaces (or APIs).[27] APIs enable communication between computer applications by setting out data available for retrieval and how it can be retrieved,[28] and "enable a software application to directly use the data it needs."[29] APIs are not new and they have been "used for decades, particularly in the United States."[30] APIs are

---

23. Regulation (EU) 2016/679, of the European Parliament and of the Council of April 27 2016, on the Protection Of Natural Persons with regard to the Processing Of Personal Data and on the Free Movement of such Data, and repealing Directive 95/46/EC (General Data Protection Regulation), art. 20, 2016 O.J. (L 119) 45 [hereinafter GDPR] (including a general right for the individual to require the transfer of their personal information in a "structured, commonly used and machine-readable format").

24. Olaf Sleijpen, *How to Make Open Finance a Success: Lessons from PSD2*, Keynote Speech at the DeNederlandscheBank 4th Annual Conference on FinTech and Regulation, Brussels (Mar. 3, 2020) ("Standardized third party access to data is vital for avoiding fragmentation."). *See* Oscar Borgogno & Giuseppe Colangelo, *Data Sharing and Interoperability: Fostering Innovation and Competition Through APIs*, 35(5) COMPUT. L. & SEC. REV. 1, 14 (2019) (showing that the lack of any equivalent legal requirements in the data portability provisions of GDPR has been criticized).

25. Heike Schweitzer & Robert Welker, *A Legal Framework For Access To Data: A Competition Policy Perspective*, *in* DATA ACCESS, CONSUMER INTERESTS AND PUBLIC WELFARE 103, 123 (Ger. Fed. Ministry of Just. & Consumer Prot. & Max Planck Inst. for Innovation & Competition ed., 2021) (finding that open banking "goes significantly beyond the 'simple' data portability right as laid down by Article 20 GDPR"). *See* Christian Reimsbach-Kounatze, *Enhancing Access to and Sharing of Data: Striking the Balance Between Openness and Control Over Data*, *in* DATA ACCESS, CONSUMER INTERESTS AND PUBLIC WELFARE 51 (Ger. Fed. Ministry of Just. & Consumer Prot. & Max Planck Inst. for Innovation & Competition ed., 2021).

26. *See* Giuseppe Colangelo & Oscar Borgogno, *Data, Innovation and Competition in Finance: The Case of the Access to Account Rule*, 31 EUR. BUS. L. R. 573 (2020).

27. *See* Borgogno & Colangelo, *supra* note 24.

28. "They are sets of protocols which define how software components communicate with one another." *Id*. at 6. Julian Cork, *Banking as a Platform*, *in* THE BOOK ON OPEN BANKING: A SERIES OF ESSAYS ON THE NEXT EVOLUTION OF MONEY 85, 88 (2018) ("the 'Babel Fish' for financial communications").

29. *See* Reimsbach-Kounatze, *supra* note 25, at 51.

30. Laura Brodsky & Liz Oakes, *Data Sharing and Open Banking*, MCKINSEY 2 (July 2017), https://www.mckinsey.com/~/media/McKinsey/Industries/Financial%20Services/Our%20Insights/Data%20sharing%20and%20open%20banking/Data-sharing-and-open-banking.pdf [https://perma.cc/8WG9-LYZV].

considered to be the most reliable technological foundation for open banking,[31] and are fundamental to the customer protection objectives of open banking. As a result, the use of standardized APIs is "an integral part of current open banking initiatives,"[32] and regarded as "critical to ensure adequate levels of interoperability for Open Banking to thrive."[33] In fact, APIs are so commonly used withopen banking that it is sometimes referred to as "open API."[34] However, open banking is not based on the use of a specific technology, and the use of APIs ensures that open banking is not confined to the use of any particular technology platform.

2. Customer Autonomy

Open banking gives customers rights to enable their customer data to be accessible and sharable, which is a form of data autonomy.[35] It can be likened to concepts of data sovereignty,[36] or informational self-determination.[37] However, customer autonomy in open banking differs from these concepts,[38] and concepts of data ownership,[39] as its purpose is to enable the customer to control their choice to share data and the use of the data which they choose to share, but it does not seek to control or exclude the use by others who receive the data through some other means.

---

31. Borgogno & Colangelo, *supra* note 24, at 8.

32. *See* Nicholls, *supra* note 13, at 122; *see also* Johannes Ehrentraud et al., *Policy Responses to Fintech: A Cross-Country Overview*, BANK FOR INT'L SETTLEMENTS: FIN. STABILITY INST. 33 (Jan. 2020), https://www.bis.org/fsi/publ/insights23.pdf [https://perma.cc/DUX5-QD9D]; *Report on Open Banking and Application Programming Interfaces*, *supra* note 10, at 15.

33. Borgogno & Colangelo, *supra* note 26, at 3; *see also* Cesare Fracassi & William J. Magnuson, *Data Autonomy*, 74 VAND. L. REV. 327, 345 (2021).

34. Such as in Singapore and Hong Kong, see *supra* note 18.

35. Fracassi & Magnuson, *supra* note 33, at 333.

36. *See* Simonetta Vezzoso, Data Portability: Initial Reflections on an Ex Ante Approach (Mar. 26, 2020), *available at* SSRN, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3561413 [https://perma.cc/EU72-7TM5].

37. Nadezhda Purtova, *Default Entitlements in Personal Data in the Proposed Regulation: Informational Self-Determination Off the Table . . . And Back On Again?*, 30(1) COMPUT. L. & SEC. REV. 6 (2014).

38. Data portability under GDPR "strives to protect the data subject's 'informational autonomy' and continued control over his or her personal data" rather than seeking to address a market failure or informational asymmetry. Schweitzer & Welker, *supra* note 25, at 120.

39. Fracassi and Magnusson argue that a data subject "owning" their data is a necessary part of data autonomy. Fracassi & Magnuson, *supra* note 33, at 345. However, defining the concept of property rights in data is difficult, partly because the essential feature of a right to exclude others is rarely able to be established. Nadezhda Purtova, *The Illusion of Personal Data as No One's Property*, 7 L. INNOVATION & TECH. 1, 7 (2015); Reimsbach-Kounatze, *supra* note 25, at 30; Bertin Martens, *An Economic Perspective on Data and Platform Market Power* 5 (Euro. Comm'n, Joint Rsch. Ctr. Digit. Econ. Working Paper No. 2020-09, 2021) ("There are no general data ownership rights in the EU or elsewhere.").

Customer autonomy in open banking is supported by the legal rights of customers to share their data.[40]

3. Recipient Accountability

Open banking makes the recipients of shared customer banking data accountable to customers for the use of the customer's data and it is a common requirement that the data shared can only be used for the purposes to which the customer has expressly consented.[41] Whilst accountability in open banking can be based on the principles from data protection laws,[42] it differs from the accountability customarily imposed by those laws. This is because the focus of accountability in open banking is to enable value to be provided to the customer through the provision of a particular good or service, rather than the protection of fundamental rights of privacy,[43] or general rights of control.[44] Recipient accountability is supported by the legal responsibilities of recipients of customer data under open banking.[45]

These three functions are fundamental to the effectiveness of open banking in achieving its objectives, analyzed next.

B. *Objectives of Open Banking*

There are high expectations for open banking. According to the BIS, open banking could change the traditional business model of banking,[46] and according to the Bank of England, open banking could change the relationship between bank and customer and "revolutionise how customers manage their finances."[47] Other claims have been more ebullient, declaring open banking to be "the first significant attempt to

40. *See* Scott Farrell, *Designing Data Rights For Canadian Open Banking: Lessons From Australian and U.K. Banking Law* (2022) (article submitted for publication) (on file with author).

41. *See generally* Inge Graef, Martin Husovec & Nadezhda Purtova, *Data Portability and Data Control: Lessons for an Emerging Concept in EU Law*, 19(6) GER. L. J. 1359 (2018).

42. *See* BANK FOR INT'L SETTLEMENTS, *supra* note 10, at 14.

43. *See* Laura Somaini, *The Right to Data Portability and User Control: Ambitions and Limitations*, 3 MEDIALAWS 164 (2018); Jörg Hoffmann, *Sector-Specific (Data-) Access Regimes of Competitors*, 33 MAX PLANCK INST. FOR INNOVATION & COMPETITION RESEARCH PAPER 343, 372 (2020).

44. *See* Oscar Borgogno & Giuseppe Colangelo, *Consumer Inertia and Competition-Sensitive Data Governance: The Case of Open Banking*, 9 J. EUR. CONSUMER & MKT. L. 143, 144 (2020).

45. *See* Scott Farrell, *Embedding Open Banking In Banking Law: Responsibilities, Performance, Risk and Trust*, 17 J. BUS. & TECH. L. 265 (2022).

46. BANK FOR INT'L SETTLEMENTS, *supra* note 10, at 9.

47. BANK OF ENG., FUTURE OF FINANCE. WHAT IT MEANS FOR THE U.K. FINANCIAL SYSTEM 105 (June 2019).

use technology to rebalance markets in favour of consumers,"[48] to create "a new paradigm"[49] to "usher in an entirely new financial services ecosystem,"[50] to "create new roles and business models in the banking sector,"[51] and "to be the next wave of digital transformation in the financial sector."[52] Although this Article does not seek to substantiate these claims, the objectives of open banking inform the requirements for participation in open banking systems. For these purposes, the objectives expressed in the different jurisdictions implementing open banking can be distilled into four key components: (1) improving competition; (2) encouraging innovation; (3) fostering inclusion; and (4) consumer protection.

1. Improving Competition

In most jurisdictions a primary objective of open banking is to improve competition in banking services. This includes the U.S., where it offers the promise of "increased competition in the provision of financial services to consumers,"[53] the U.K. where, by increasing rivalry between banks,[54] it is intended to remedy the problem "that older and larger banks do not have to compete hard enough for customers" business, and smaller and newer banks find it difficult to grow,[55] and Australia, where it is intended to "transform the competitive landscape in financial services."[56]

---

48. OPEN DATA INST. & FINGLETON, OPEN BANKING, PREPARING FOR LIFT OFF 4 (2019), https://www.openbanking.org.U.K./wp-content/uploads/open-banking-report-150719.pdf [https://perma.cc/A8Z5-XBHU].

49. Zunzunegui, *supra* note 21, at 15.

50. Brodsky & Oakes, *supra* note 30, at 1.

51. Gozman, Hedman & Olsen, *supra* note 13, at ⁋ 6.

52. MICROSOFT, LINKLATERS & ACCENTURE, OPEN BANKING: A SHARED OPPORTUNITY 3 (Report, 2019).

53. Bureau of Consumer Fin. Prot., Consumer Access to Financial Records, 85 Fed. Reg. 71,005 (proposed Nov. 6, 2020).

54. Competition & Mkts. Auth., *Retail Banking Market Investigation*, GOV.U.K. ⁋ 13.6 (Final Report, Aug. 9, 2016), https://assets.publishing.service.gov.U.K./media/57ac9667e5274a0f6c00007a/retail-banking-market-investigation-full-final-report.pdf [https://perma.cc/8CK3-2LUZ]. *See also* Fin. Conduct Auth., *Open Finance* ⁋ 1.4 (Feedback Statement No. FS21/7, Mar. 2021), https://www.fca.org.U.K./publication/feedback/fs21-7.pdf [https://perma.cc/M88G-2BKQ]; Colangelo & Borgogno, *supra* note 26, at 573.

55. Press Release, Competition & Mkts. Auth., *CMA Paves the Way for Open Banking Revolution* (Aug. 9, 2016), https://www.gov.U.K./government/news/cma-paves-the-way-for-open-banking-revolution [https://perma.cc/S2RP-Y5SK].

56. Media Release, Scott Morrison, Treasurer, *Government Response to the Open Banking Review* (May 9, 2018), https://ministers.treasury.gov.au/ministers/scott-morrison-2015/media-releases/government-response-open-banking-review [https://perma.cc/4XTZ-TYL4].

The use of open banking for this purpose arises from recognition that "banking has a competition problem,"[57] which more customary competition regulatory methods have not been effective to remedy.[58] Open banking seeks to address this problem through the central role of customer account information in banking.[59] Banks rely on this information to assess, manage and price credit risk.[60] Because of its importance, banks control access to customer account information and, in doing so, perform a "gatekeeper role."[61] This represents a substantial advantage to banks in providing financial services,[62] and a barrier to entry to other competitors, including start-up financial technology firms (or fintechs) seeking to offer competing financial services to banks' customers.[63] This is known as the "data bottleneck problem,"[64] and it leads to market failures in banking competition such as information asymmetry and high search and switch costs.[65]

The sharing of data enabled by open banking can mitigate this problem by reducing barriers to entry and expansion.[66] Enabling customers to share their account data with alternative providers can reduce the associated switching costs and the "lock-in" to current service

57. *See* sources cite *supra* note 33.

58. "[T]he antitrust enforcement toolbox is inadequate to tackle effectively the need to ensure access to data." Borgogno & Colangelo, *supra* note 24, at 6. "[I]t can be invoked only to gain access to a dataset held by a dominant firm, on a case-by-case basis." Colangelo & Borgogno, *supra* note 26, at 7; s*ee also* Vezzoso, *supra* note 36.

59. "[T]he entire sector hinges on the re-use of account and transaction information." *See* Borgogno & Colangelo, *supra* note 44.

60. "[B]anks' core business is processing data." Julio Martinez, *Open Banking and the Role of Banks*, *in* THE BOOK ON OPEN BANKING: A SERIES OF ESSAYS ON THE NEXT EVOLUTION OF MONEY 72, 74 (2018).

61. Borgogno & Colangelo, *supra* note 44.

62. *See* Christine A. Parlour, Uday Rajan & Haoxiang Zhu, *When Fintech Competes For Payment Flows* (Apr. 1, 2020), SSRN https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3544981 [https://perma.cc/ZE99-XGM7].

63. Colangelo & Borgogno, *supra* note 26. This concern is not limited to banking. *See* Simonetta Vezzoso, *The Dawn of Pro-Competition Data Regulation for Gatekeepers in the EU*, 17(2) EURO. COMPETITION J. 1 (2021).

64. Borgogno & Colangelo, *supra* note 26, at 3.

65. Fracassi & Magnuson, *supra* note 33, at 327, 344.

66. *See* AUSTL. COMPETITION & CONSUMER COMM'N, DIGITAL PLATFORMS INQUIRY: FINAL REPORT 115 (2019); Jan Krämer & Daniel Schnurr, *Big Data and Digital Markets Contestability: Theory of Harm and Data Access Remedies*, 18 J. COMPETITION L. & ECON. 255, 289 (2021) ("The unique characteristic of data as a bottleneck resource, as opposed to material bottleneck resources, is its nonrivalrous nature. Thus, the bottleneck can in principle be resolved by enabling nonexclusive access to it."). *See also Annual Economic Report* (Bank for Int'l Settlements, Basel, Swtiz), June 30, 2019, at 67, https://bis.org/publ/arpdf/ar2019e.pdf [https://perma.cc/JD68-Z3NT].

providers.[67] Providing customers with easy access to their banking data enables them to "shop around,"[68] and overcomes the "traditional customer inertia" in retail banking.[69] By mitigating the information asymmetry problems which have traditionally impacted banking,[70] open banking seeks to increase competition on the "merits" in banking, particularly because banking is increasingly "powered by data-based technologies,"[71] resulting in "more cost-effective banking and increased competitiveness in financial markets."[72]

2. Encouraging Innovation

Encouraging innovation is fundamental to the benefits of the new, competitive financial services intended to be provided through open banking. Improving financial products and services through innovation is a stated goal of open banking in the U.S.,[73] and innovation has been an important purpose of open banking in the EU, where it is to "allow for the development of user-friendly, accessible and innovative means of payment,"[74] in the U.K.,[75] and in Australia, where it is to "provide a framework from which new ideas and business can emerge and grow."[76] The focus on enabling innovation means that "[o]pen banking is one of the rare cases globally where regulation precedes innovation and not vice versa."[77]

---

67. *See* Borgogno & Colangelo, *supra* note 26, at 6. *See also* Peter Swire & Yianni Lagos, *Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy Critique*, 72 MD. L. REV. 335, 338 (2012).

68. Oscar Borgogno & Giuseppe Colangelo, *The Data Sharing Paradox: BigTechs in Finance*, 16 EUR. COMPETITION J. 492, 4 (2020).

69. Michael McKee, Chris Whitaker & Neil Millar, *PSD2 and Open Banking - Rewiring the Plumbing of the European Payments Ecosystem*, 35 J. INT'L BANKING L. & REGUL. 85, 86 (2020). *See also* Borgogno & Colangelo, *supra* note 44, at 2–3.

70. Colangelo & Borgogno, *supra* note 26, at 4.

71. Vezzoso, *supra* note 36, at 18.

72. Bruno Zeller & Andrew M. Dahdal, *Open Banking and Open Data in Australia: Global Context, Innovation and Consumer Protection* 21 (Qatar Univ. Coll. of L., Working Paper No. 2021/001, 2021).

73. *See* Consumer Access to Financial Records, 85 Fed. Reg. 71,003 (proposed Nov. 6, 2020); Exec. Order No. 14,036, 86 Fed. Reg. 36,987 (July 9, 2021) ("Promoting Competition in the American Economy").

74. Directive, art. 98(2)(e),2015/2366 of the European Parliament and of the Council of 25 November 2015 on Payment Services in the Internal Market, Amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation No 1093/2010, and Repealing Directive 2007/64/EC, 2015 O.J. (L 337) 35, 107 [hereinafter PSD2].

75. *See* HM TREASURY, DATA SHARING AND OPEN DATA IN BANKING: RESPONSE TO THE CALL FOR EVIDENCE 3 (2015).

76. COMMONWEALTH TREASURY, CONSUMER DATA RIGHT 1 (2018).

77. Pinar Ozcan & Markos Zachariadis, *Transformation: Lessons Learned From Implementing PSD2 In Europe* 3 (SWIFT Inst. Working Paper No. 2017-006, 2021).

Open banking is designed to be a key enabler of fintech innovation,[78] to "facilitate the growth of a dynamic intermediary sector . . . with the ability and incentive to help customers,"[79] using "innovative aftermarkets services" that rely on access to account data.[80] This innovation is driven by the increased accessibility of customer account data. This data "represent[s] an extremely valuable raw material for the provision of new services,"[81] and the sharing of customer data allows banking services to be "unbundled" so that customers can, for example, separate the taking of their deposits and the organization of their payments.[82] This permits customers to make different choices in respect of each unbundled element and permits greater efficiency to be obtained. This is hoped to enable the creation of new business models in banking.[83]

3. Fostering Inclusion

Jurisdictions such as Mexico, Brazil and India have undertaken open banking for the express purpose of improving financial inclusion.[84] The increased competition and innovation from enabling access to customer data is intended to empower new entrants in the market to create new products and services which are adapted to the needs of those who are underserved by existing providers.[85] The potential for servicing underserved and unserved customers increases if customer data beyond banking, such as utility and telecommunications data, are included to complement the insufficiently reliable traditional assessments of credit

78. FinTech Austl., *Senate Issues Paper Response* (Submission Paper, Austl. S. Select Comm. Inquiry of Fin. Tech. & Regul. Tech., Dec. 2019).

79. COMPETITION & MKTS. AUTH., RETAIL BANKING MARKET INVESTIGATION FINAL REPORT 443 (2016).

80. Schweitzer & Welker, *supra* note 25, at 123.

81. Borgogno & Colangelo, *supra* note 44, at 7.

82. BANK FOR INT'L SETTLEMENTS, *supra* note 10, at 8. *See also* Markos Zachariadis and Pinar Ozcan, *The API Economy and Digital Transformation in Financial Services: The Case of Open Banking* 3 (SWIFT Inst. Working Paper No. 2016-001, 2017).

83. Gozman, Hedman & Olsen, *supra* note 13, at 10. *See also* AUSTL. COMPETITION & CONSUMER COMM'N, *supra* note 66, at 11.

84. Ariadne Plaitakis & Stefan Staschen, *Open Banking: How to Design for Financial Inclusion* 6 (Oct. 2020) (unpublished working paper) (on file with C.G.A.P.).

85. "The global evidence we reviewed suggests that, by responsibly using shared customer transaction data, fintechs and other types of financial institutions in [emerging and developing economies] may be able to do a better job than traditional banks have done with such data." *Id*. at 8; *see also* David Beardmore, Claudia May Del Pozo, et al., *What is the potential for open banking in Mexico?*, C MINDS (Apr. 27, 2018), https://cminds.pubpub.org/pub/openbankingmx/release/1.

worthiness.[86] This is intended to foster credit inclusion and lower financial inequalities.[87]

Also, open banking is hoped to provide financial inclusion benefits by enabling improvement in financial management, particularly through sharing data with trusted intermediaries.[88] This is not limited to emerging economies. In the U.K., open banking has led to services that can identify upcoming bills and allocate funding from inexpensive sources rather than overdrafts, and services that can alert friends and family to help a consumer in financial difficulties.[89] Financial inclusion has also been an important consideration in the design of open banking in Canada,[90] and developments to enable further inclusion have been recommended in Australia.[91] Similar desire for inclusion can be seen in the U.S. with the instructions given by Congress to the CFPB to implement and enforce consumer law "for the purpose of ensuring that all consumers have access to markets for consumer financial products and services."[92]

4. Consumer Protection

The primary consumer protection objective of open banking is achieved by its use as a safer alternative to the other methods already used by customers to share banking data. This has been a key factor in its adoption in Canada,[93] India,[94] and in the U.K. and EU.[95] Until the introduction of open banking and the use of APIs for the sharing of

86. Leena Datwani & Anand Raman, *India's New Approach to Personal Data-Sharing* (C.G.A.P., Working Paper, July 2020). *See also* Yan Carriere-Swallow, Vikram Haksar & Manasa Patnam, *India's Approach to Open Banking: Some Implications for Financial Inclusion International Monetary Fund* (IMF Working Paper Feb. 2021); Plaitakis & Staschen, *supra* note 84, at 2.

87. Colangelo & Borgogno, *supra* note 26, at 21.

88. Plaitakis & Staschen, *supra* note 84.

89. HM Gov't, *Smart Data: Putting Consumers in Control of their Data and Enabling Innovation* (Consultation Paper, June 2019). *See also* DEP'T OF FIN. CAN., CONSUMER-DIRECTED FINANCE: THE FUTURE OF FINANCIAL SERVICES (Feb. 2020).

90. *See* ADVISORY COMM. ON OPEN BANKING, FINAL REPORT OF ADVISORY COMMITTEE ON OPEN BANKING (Apr. 2021); DEP'T OF FIN. CAN., *supra* note 89.

91. *See* COMMONWEALTH TREASURY, INQUIRY INTO FUTURE DIRECTIONS FOR THE CONSUMER DATA RIGHT: GIVING CONSUMERS CHOICE, CONVENIENCE AND CONFIDENCE 171 (Oct. 2020). The author led this inquiry.

92. Dodd-Frank Act § 1021, 12 U.S.C. § 5511 (2010).

93. Dep't of Fin. Can., *Minister Morneau Announces Second Phase of Open Banking Review with a Focus on Data Security in Financial Services* (News Release, Jan. 31, 2020).

94. "Where models for digital sharing exist, they typically involve transferring data through intermediaries that are not always secure or through specialized agencies that offer little protection for customers." Datwani & Raman, *supra* note 86, at 6.

95. Through the mandatory requirements for "Strong Customer Authentication." McKee, Whitaker & Millar, *supra* note 69, at 86. *See also* Simonetta Vezzoso, *Fintech, Access to Data, and the Role of Competition Policy*, *in* COMPETITION AND INNOVATION at 32, 34 (V. Bagnoli ed., 2018).

customer banking data, customers would most likely provide their online banking login credentials to those with whom they wanted to share their banking information.[96] This process is commonly known as "screen scraping" and it is a controversial method of accessing customer account data,[97] although it remains commonly used.[98] Screen scraping is argued to be a slow and unstable technology with potential inaccuracies in the data collected (due to the lack of standardization in the bank interfaces being "scraped"),[99] which exposes customers to increased cyber-security risk,[100] and increases the opportunity to take advantage of vulnerable customers and cause financial hardship.[101] Open banking using APIs avoids these risks as customer credentials are only shared with their bank.[102] In the U.S., the CFPB noted that all participants at a symposium on Consumer Access to Financial Records agreed that a move away from screen scraping "would benefit consumers and all market participants."[103]

Open banking frameworks also have other consumer protection objectives such as improving consumers' comprehension of the risks and benefits in sharing their data. This aspect of consumer protection is a key

96. *See* Hoffmann, *supra* note 43; Vezzoso, *supra* note 95, at 35.

97. *See* SELECT COMM. ON FIN. TECH. & REGUL. TECH. (AUSTL.), SEN., INTERIM REPORT (Sept. 2020); Memorandum from H.R COMM. ON FIN. SERV., 117TH CONG., PRESERVING THE RIGHT OF CONSUMERS TO ACCESS PERSONAL FINANCIAL DATA (2021).

98. "Four million Canadian consumers are already taking control by using screen scraping apps offered by fintech companies in order to meet their needs for a more personalized, convenient digital banking experience." STANDING SENATE COMM. ON BANKING TRADE & COM., OPEN BANKING: WHAT IT MEANS FOR YOU 37 (June 2019).

99. This results in no guarantee of data currency or accuracy. *See* Han-Wei Liu, *Shifting Contour of Data Sharing in Financial Market and Regulatory Responses: The U.K. and Australian Models*, 10 AM. UNIV. BUS. L. REV. 287, 293 (2021).

100. Screen scraping can raise other legal concerns, such as unauthorized access under cybercrime legislation, copyright infringement, misleading and deceptive conduct, and trespass to goods. *See* Trevor Jeffords, *What is "Screen Scraping" and Is It Lawful in Australia?*, 44 J. AUSTL. & N.Z. SOC. COMPUT. & L. 24, 24 (2001). *See also* hiQ Labs, Inc. v. LinkedIn Corp., 938 F.3d 985 (9th Cir. 2019).

101. SELECT COMM. ON FIN. TECH. & REGUL. TECH. (AUSTL.), *supra* note 97. Screen scraping is commonly used in the United States "where screen-scrapers have even been known to sell customer data to hedge funds." GOTTFRIED LEIBBRANDT & NATASHA DE TERAN, THE PAY OFF: HOW CHANGING THE WAY WE PAY CHANGES EVERYTHING 158 (2020).

102. For this reason, banks prefer the use of open banking to screen scraping. BANK FOR INT'L SETTLEMENTS, *supra* note 10, at 6.

103. *See* CONSUMER FINANCIAL PROTECTION BUREAU, CFPB SYMPOSIUM: CONSUMER ACCESS TO FINANCIAL RECORDS (Feb. 26, 2020), https://www.consumerfinance.gov/about-us/events/archive-past-events/cfpb-symposium-consumer-access-financial-records/ [https://perma.cc/3RMG-GLKD]. *See also* the comment letters on the ANPR: REGULATIONS.GOV, Comments to *Consumer Access to Financial Records* (Nov. 6, 2020), https://www.regulations.gov/document/CFPB-2020-0034-0001/comment [https://perma.cc/5X43-DA68] (last visited July 18, 2021).

objective of Australian open banking,[104] and in the EU.[105] In addition, the greater accessibility of data has the effect of enhancing the bargaining power of consumers which can also be regarded as "a new frontier of consumer protection policy."[106]

C. *Foundations of Participation in Open Banking Systems*

Achievement of these objectives of open banking requires communication of customer data at scale, beyond small numbers of bilateral exchanges, involving many customers, many banks and many recipients.[107] Such broad participation encourages competition by increasing the contestability of banking services, improves innovation by enabling collaboration in the development of banking products, fosters inclusion by facilitating increased access to trusted intermediaries for vulnerable customers, and enhances consumer protection by increasing the number of participants who can identify safety issues in open banking as they arise. Two foundations are critical to enabling the benefits of participation to be realized: enabling access and preserving stability.

1. Enabling Access to Participation in Open Banking Systems

The breadth of participation required for open banking to achieve its objectives is fundamentally connected with it becoming "a large innovative ecosystem."[108] In the U.K., the creation of a "vibrant ecosystem" in open banking has been found to be critical due to "the benefits it generates for people, businesses and the wider economy in helping to open up competition and forge the way for new services to be offered, continues to thrive and develop."[109] In Australia, the benefits of open banking have been found to be "intrinsically linked to establishing a vibrant ecosystem of accredited data recipients (ADRs) and other participants."[110] In the United States, the need for such participation is also recognized, with the CFPB making numerous references to "ecosystem participants" in its' ANPR.[111]

---

104. "Consumer protection is the ultimate goal of the Australian CDR Regime." Zeller & Dahdal, *supra* note 72, at 19.

105. PSD2, *supra* note 74, at recital 6.

106. Colangelo & Borgogno, *supra* note 26, at 21.

107. *See* Open Banking Implementation Entity, *Real Demand for Open Banking as User Numbers Grow to More Than Two Million* (Sept. 28, 2020), https://www.openbanking.org.U.K./news/real-demand-for-open-banking-as-user-numbers-grow-to-more-than-two-million/ [https://perma.cc/AFZ8-DKHV].

108. OPEN DATA INST. & FINGLETON, *supra* note 48, at 35.

109. COMPETITION & MKTS AUTH., *supra* note 10.

110. Exposure Draft Explanatory Materials, Competition and Consumer (Consumer Data Right) Amendment Rules (No. 1) 2021 (Sept. 30, 2021), https://www.legislation.gov.au/Details/F2021L01392 [https://perma.cc/5MA6-XMLS].

111. There are 26 references to "ecosystem" in the 33 pages of text in the ANPR.

Access to participation in an open banking ecosystem is not limited to the direct participation of customers, banks, and data recipients. To provide data-driven innovations, data recipients are likely to choose or need to use agents, intermediaries, and outsourced service providers. This creates interdependence between specialized and differentiated participants as each relies on the services and data being provided by others. Further, as noted in the ANPR, a key feature of this participation is that different participants can perform differing or multiple roles.[112] Also, the requirements of direct participation could be difficult for emerging entities with more limited resources whose involvement could contribute significantly to competition and innovation goals. Providing access to these entities requires facilitation of indirect participation, whilst maintaining sufficient accountability for those receiving customer data. Through this development, open banking systems become "multiagent and distributed systems interacting in parallel, rather than individual agents related by simple, sequential channels of communication,"[113] also known as multilateral networks. Progress in the U.K. is already described in this way:

> The Open Banking ecosystem in the U.K. now extends far beyond the CMA9—currently comprising more than 330 regulated firms made up of over 230 third party providers of services and more than 90 payment account service providers who together account for over 95% of current accounts. Moving forward, it will be critical that this vibrant ecosystem and the benefits it generates for people, businesses, and the wider economy in helping to open up competition and forge the way for new services to be offered, continues to thrive and develop.[114]

And the Australian open banking system is intended to

> connect more customers, data holders and data recipients, linked by their participation in a system with set rules and standards. Customers will develop relationships with both data holders and data recipients. Sometimes these connections will be strengthened by some parties performing more than one role. The connections and network effects should increase . . . [and] [a]s the connections increase, a

112. Bureau of Consumer Fin. Prot., Consumer Access to Financial Records, 85 Fed. Reg. 71,003 (proposed Nov. 6, 2020). https://www.federalregister.gov/documents/2020/11/06/2020-23723/consumer-access-to-financial-records [https://perma.cc/4KJY-MEZ3].

113. LUCIANO FLORIDI, INFORMATION: A VERY SHORT INTRODUCTION 53 (2010). Herbert Zech, *Data as a Tradeable Commodity–Implications for Contract Law*, *in* PROCEEDINGS OF THE 18TH EIPIN CONGRESS: THE NEW DATA ECONOMY BETWEEN DATA OWNERSHIP, PRIVACY AND SAFEGUARDING COMPETITION 3 (Josef Drexl ed., 2017).

114. COMPETITION & MKTS. AUTH., *supra* note 10.

> data ecosystem should naturally grow in a similar way to the ecosystems in other markets where unique functions may be performed by specialist service providers, enabling a wider range of higher quality and more cost-effective services. Specialization may manifest in the regime in a number of different ways including through the presence of software providers, software-as-a-service, outsourced service providers, arm's length businesses working cooperatively and arm's length businesses operating independently but in complementary ways.[115]

2. Preserving Stability of Participation in Open Banking Systems

Even regulated open banking systems, like those in Australia and the U.K., do not prescribe the connections which new participants create with existing participants. As in other information services, this could result in many recipients of customer data relying on the services of a limited number of providers, who could be data recipients themselves. Some participants, such as those who offer technology-based services to other participants as well as customers, might have "an unprecedented number of connections."[116] Evidence of this interconnectedness is already emerging in U.K. open banking. The Open Banking Implementation Entity (OBIE) announced that up to one half of small to medium-sized enterprises in the U.K. utilize U.K. open banking, most often in relation to online accounting services,[117] and a single data recipient in the U.K. framework which provides connectivity services to others already claims that one-half of all 'open banking traffic' in U.K. open banking flows through their platform.[118] Further, both Australia and the U.K. enable participants to outsource functions to a limited number of global cloud storage providers.[119]

---

115. COMMONWEALTH TREASURY, *supra* note 91, at 106.

116. B.S. MANOJ, ABHISHEK CHAKRABORTY & RAHUL SINGH, COMPLEX NETWORKS: A NETWORKING AND SIGNAL PROCESSING PERSPECTIVE 177 (2018).

117. Open Banking Implementation Entity, *Adapting to Survive: U.K.'s Small Businesses Leverage Open Banking as Part of Their Covid-19 Crisis Recovery* (Press Release, Dec. 7, 2020), https://www.openbanking.org.U.K./news/adapting-to-survive-uks-small-businesses-leverage-open-banking-as-part-of-their-covid-19-crisis-recovery/ [https://www.openbanking.org.U.K./news/adapting-to-survive-uks-small-businesses-leverage-open-banking-as-part-of-their-covid-19-crisis-recovery/].

118. *TrueLayer Raises $70m to Build the World's Most Valuable Open Banking Network*, BUSINESS WIRE (Apr. 8, 2021), https://www.businesswire.com/news/home/20210408005064/en/TrueLayer-Raises-70m-to-Build-the-World's-Most-Valuable-Open-Banking-Network [https://perma.cc/B685-5NM7]. *See also* We're Open Banking Experts, TRUELAYER (2021), https://truelayer.com [https://perma.cc/HPV5-SWH8].

119. *See infra* Part IV.C.

This is likely to result in open banking systems becoming "complex systems"[120] of interdependencies where some participants are highly connected whilst others are not.[121] An important feature of such systems is that they can be both robust and fragile,[122] depending on the connectivity of a participant that fails. If a highly connected participant were to suddenly cease to provide open banking services, then not only might their customers suffer an interruption in their own business (which might provide services to others too), but also other data recipients may not be able to provide their own services. Also, if such a participant were to be subject to a cyber-attack which spread from their systems to others, then they could cause widespread damage due to their connectivity.[123] As with other complex systems, unless appropriately managed, the interdependence created in open banking by multilateral participation could lead to "cascading failures," "breakdown avalanches," "domino effects," or "systemic failure."[124]

Of particular importance in this regard is the impact on the confidence and trust in open banking. Trust and confidence are core features in the design of open banking,[125] and are recognized to be crucial factors in its success.[126] "[C]onsumer trust in the system underpins participation and can be lost quickly if something goes wrong."[127] Accordingly, as open banking develops into the innovative ecosystem required to achieve its

120. Charalampos Sergiou et al., COMPLEX SYSTEMS: A COMMUNICATION NETWORKS PERSPECTIVE TOWARDS 6G, 8 IEEE ACCESS 89007 (2020). *See also* PAVLOS ANTONIOU & ANDREAS PITSILLIDES, UNDERSTANDING COMPLEX SYSTEMS: A COMMUNICATION NETWORKS PERSPECTIVE (Dept. of Comput. Sci., Univ. of Cyprus, 2007).

121. GUIDO CALDARELLI & MICHELE CATANZARO, NETWORKS: A VERY SHORT INTRODUCTION 17 (2012); BANK FOR INT'L SETTLEMENTS, COMM. ON PAYMENT & SETTLEMENT SYS., CORE PRINCIPLES FOR SYSTEMICALLY IMPORTANT PAYMENT SYSTEMS ¶ 2.1 (Jan. 2001). *See also* the seminal work in this area: Albert-László Barabási & Réka Albert, EMERGENCE OF SCALING IN RANDOM NETWORKS, 286 SCI. 509 (1999).

122. STEPHEN MILLARD, ANDREW HALDANE & VICTORIA SAPORTA, THE FUTURE OF PAYMENT SYSTEMS 249 (2007).

123. ADVISORY COMM. ON OPEN BANKING, *supra* note 90.

124. CALDARELLI & CATANZARO, *supra* note 121.

125. OPEN DATA INST. & FINGLETON, *supra* note 48, at 25.

126. *See* Michiel Bijlsma, Carin van der Cruijsen & Nicole Jonker, *Consumer Propensity to Adopt PSD2 Services: Trust for Sale?* (DeNederlandscheBank Working Paper No. 671, Jan. 2020). *See also* GOZMAN, HEDMAN & OLSEN, *supra* note 13; Faith Reynolds et al., *Consumer Priorities for Open Banking* (June 2019), https://www.openbanking.org.U.K./wp-content/uploads/Consumer-Priorities-for-Open-Banking-report-June-2019.pdf [https://perma.cc/2HJE-GMAH]; Ine van Zeeland & Jo Pierson, *In Banks We Trust: Banks as Custodians of Personal Data in Open Banking Ecosystems* (July 30, 2021), available at https://papers.ssrn.com/sol3/papers.cfm? abstract_id=3896405 [https://perma.cc/A8JQ-Y6CT]; Consumer Pol'y Rsch. Centre, *Stepping Towards Trust* (Aug. 2020), https://consumerdatastandards.gov.au/sites/consumerdatastandards.gov.au/files/uploads/2020/09/20200902_CPRC-Report-1_Publication.pdf [https://perma.cc/2P3Q-MV76].

127. ADVISORY COMM. ON OPEN BANKING, *supra* note 90, at 20.

objectives, it needs to increase in credibility and grow to be trusted, so that customers and participants participate based on "confident reliance" on the performance of the system as a whole.[128] Such "impersonal,"[129] "systemic,"[130] or "institutional"[131] trust can develop in open banking from the involvement of "a range of interacting and interdependent actors . . . operating within organizations and broader systems and subsystems that govern transactions, standards, licensing and enforcement of laws and regulation,"[132] and from the safe provision of services to customers by 'a chain of strangers.'[133] In other words, it can emerge from success of open banking in developing as a safe multilateral network and complex system.

However, trusted systems can lose their credibility quickly because the foundation is past performance and an expectation of the effectiveness of constraints on future performance.[134] If an open banking system fails to perform as expected, for example by the failure of a data recipient to perform its obligations to too many customers, then an "essential condition" of the confidence in it is eroded.[135] This has been described as "information contagion,"[136] and it can cause system-wide risks even in systems which otherwise would not be considered to give rise to systemic risks.[137] There is potential for this information contagion to arise in open banking as a loss of customer data by some customers could cause many others to lose confidence in the system, and withdraw from using it for data sharing. Credibility can be lost quickly in network failures and open banking systems could be particularly susceptible to a spreading loss of confidence if it is not easy for non-defaulting participants to prove that they are complying with their data-related obligations.[138]

---

128. Nicole Gillespie & Robert Hurley, *Trust and the Global Financial Crisis*, *in* HANDBOOK OF ADVANCES IN TRUST RESEARCH 177, 178 (Reinhard Bachmann & Akbar Zaheer eds., 2013).

129. Susan P. Shapiro, *The Social Control of Impersonal Trust*, 93(3) AM. J. SOCIO. 623 (1987).

130. Felix Roth, *The Effect of the Financial Crisis On Systemic Trust*, 44 INTERECONOMICS, no. 4, 203 (2009).

131. RACHEL BOTSMAN, WHO CAN YOU TRUST?: HOW TECHNOLOGY BROUGHT US TOGETHER – AND WHY IT COULD DRIVE US APART 7 (2017) ("[A] kind of intermediated trust that ran through a variety of contracts, courts and corporate brands, freeing commerce from local exchanges and creating the foundation for an organized industrial society.").

132. Gillespie & Hurley, *supra* note 128, at 179.

133. Shapiro, *supra* note 129, at 626.

134. Timothy C. Earle, *Trust, Confidence, and the 2008 Global Financial Crisis*, 29 RISK ANALYSIS: AN INT'L J. , no. 6, 785, 786 (2009).

135. *Id*. at 788 ("Confidence is fragile" and "has a specific performance criterion.").

136. Co-Pierre Georg, *The Effect of the Interbank Network Structure on Contagion and Common Shocks*, 37 J. BANKING & FIN., no. 7, 2216, 2220 (2013).

137. MILLARD, HALDANE & SAPORTA, *supra* note 122, at 257.

138. This is explained further in Farrell, *supra* note 45.

D. *Summary*

Part I has introduced open banking and its functions, objectives and foundations of participation. It has shown that in ensuring that its functions achieve its objectives, it results in multilateral networks and complex systems with the potential for systemic risks which could cause significant harm particularly if they impair the trust and confidence in open banking. This makes the governance of access and stability in participation in open banking systems critical. Fortunately, there is a benchmark that can be used in aiding the design of legal features which provide this governance, namely banking payment systems. The basis for doing so is described in the next Part.

II. FUNCTIONAL EQUIVALENCE WITH BANKING PAYMENT SYSTEMS

Part I showed that enabling customers to communicate their banking data is fundamental to achieving the objectives of open banking. This communication is supported by the functions of data portability, customer autonomy and recipient accountability performed by open banking with respect to customer data. This Part shows that communication of customer-related banking data is also fundamental to the performance of banking payment systems, which are also supported by equivalent functions performed with respect to customer funds. Further, like open banking systems, the effectiveness of banking payment systems is also dependent on participation which is established on the foundations of enabling access and preserving stability. This functional similarity from a customer perspective and from a systemic perspective are analyzed below.

A. *Functional Equivalence from a Customer Perspective*

A primary economic function performed by commercial banks is transfer of customer funds as the customer instructs.[139] This is part of the "essence of what banks promise to their depositors,"[140] and the legal relationship between bank and customer.[141] It provides both autonomy to customers in dealing with their funds and accountability for banks that receive their customer's funds. The legislative, regulatory, contractual,

---

139. BENJAMIN GEVA, BANK COLLECTIONS AND PAYMENT TRANSACTIONS: A COMPARATIVE STUDY OF LEGAL ASPECTS 7 (2001).

140. Dan Awrey & Kristin van Zwieten, *The Shadow Payment System*, 43 J. CORP. L. 775, 783 (2017–2018).

141. *See* Foley v. Hill [1848] Eng.. Rep. 2 (HL) 28 (appeal taken from U.K.); Joachimson v. Swiss Bank Corp. (1921) 3 AC 110 (KB) (appeal taken from U.K.); Tournier v. Nat'l Provincial and Union Bank of Eng. (1924) 1 AC 461 (KB) (appeal taken from U.K.); *Laing v. Bank of N.S.W.* (1952) 54 SR (NSW) 41, 43 (Austl.); *Re Austl. and N.Z. Savings Bank Ltd.*; *Mellas v. Evriniadis* [1972] VR 690 (Vict.) (Austl.); *Smorgan v. Austl. and N.Z. Banking Group Ltd.*; *Fed. Comm'n of Tax'n v. Smorgon* (1976) 134 CLR 475 (Austl.).

and technological arrangements which enable this function to be performed have evolved over many centuries,[142] so that now most payments are funds transfers[143] effected by communicating changes to bank account data.[144] 'Nothing tangible or intangible is transferred,'[145] and instead messages or transfers of *information* cause the change in the account balances, and rules which govern them are the equivalent of delivery and possession in legal tender.[146] In fact, "[b]anks from this perspective, are specialized institutions for facilitating the transmission and recording of relevant payment information,"[147] and "information is central to the working of payment systems."[148] Accordingly, the communication of customer-related data is at the foundation of payments of customer funds through banking payment systems.[149] This forms the basis of the functional similarity between the sharing of customer data and the payment of customer funds.

The functional similarity is reinforced by the understanding that general data and customer account information are valuable.[150] Both open banking and banking payment systems involve the transfer of information of value to customers, being either customer funds or customer data. In each case, the customer can choose to transfer that value (customer autonomy), by the communication of information (data portability), and the recipient is responsible for the custody of the value

142. *See* BENJAMIN GEVA, THE PAYMENT ORDER OF ANTIQUITY AND THE MIDDLE AGES: A LEGAL HISTORY 5 (2011). "[M]odern banking in the loan and payment networks can be traced back to the Knights Templar and the Italian renaissance banks." ROSS CRANSTON ET AL., PRINCIPLES OF BANKING LAW 3 (3rd ed. 2017). Also, safekeeping functions performed by London goldsmiths developed into banking services by the late-seventeenth century. *See* Awrey & van Zwieten, *supra* note 140.

143. *See* GEVA, *supra* note 139, at 7. *See also* MILLARD, HALDANE & SAPORTA, *supra* note 122.

144. MICHAEL BRINDLE & RAYMOND COX, LAW OF BANK PAYMENTS ⁋ 3-002 (5th ed. 2018).

145. GEVA, *supra* note 142, at 607.

146. DAVID FOX, PROPERTY RIGHTS IN MONEY ¶ 3.14 (2008).

147. MILLARD, HALDANE & SAPORTA, *supra* note 122, at 68.

148. Charles M. Kahn & William Roberds, *Why Pay? An Introduction to Payments Economics*, 18(1) J. OF FIN. INTERMEDIATION 1, 13 (2009).

149. *Id*.

150. Vezzoso, *supra* note 95, at 39. *See also* Buckley et al., *supra* note 13, at 3; INT'L TELECOMM. UNION, POWERING THE DIGITAL ECONOMY, REGULATORY APPROACHES TO SECURING CONSUMER PRIVACY, TRUST AND SECURITY (2018); PRODUCTIVITY COMM. (AUSTL.), DATA AVAILABILITY AND USE (Report No. 82, 2017); Austl. Comput. Soc., *Privacy in Data Sharing: A Guide for Business and Government*, WHITE PAPER, Nov. 2018; Gianclaudio Malgieri & Bart Custers, *Pricing Privacy – The Right to Know the Value Of Your Personal Data*, 34 COMPUT. L. & SEC. REV. 289 (2018); ORG. FOR ECON. CO-OPERATION & DEV., EXPLORING THE ECONOMICS OF PERSONAL DATA: A SURVEY OF METHODOLOGIES FOR MEASURING MONETARY VALUE (2013); HM Treasury, *The Economic Value of Data*, DISCUSSION PAPER (2018); Yan Carrierie-Swallow & Vikram Haksar, *Open Banking and the Economics of Data*, *in* Jeng, *supra* note 13, at 127.

transferred (recipient accountability). In fact, 'finance, data and technology are now all tethered one to the other.'[151]

B. *Functional Equivalence from a Systemic Perspective*

The functional similarity between open banking and banking payment systems extends to the broader systemic perspective and banking payment systems share the systemic foundations to participation of access and stability.

1. Enabling Access to Participation in Banking Payment Systems

A primary function of a banking payment system is facilitating communication of payment instructions and their settlement.[152] Comprising "a network of interconnecting entities that facilitates the exchange of data required to initiate, authorize, clear, and settle cash or credit claims between payors and payees,"[153] payment systems create a "complex network of relationships and payment flows"[154] which "can be treated as a specific example of a complex network."[155] Multilateral participation is crucial because it enables the efficiency which is the economic driver of the development of payment systems.[156] Whilst bilateral fund transfers provide some efficiency benefits, these benefits are increased with the development of multilateral links in a networked payment system by reducing costs through streamlining process and standardizing relationships.[157] The use of payment systems, rather than combinations of bilateral account arrangements, is a "less costly and more secure option for banks."[158] Further efficiencies arise by reducing the liquidity that banks need to make payments, and by allowing banks to reallocate their resources to assets which produce a greater return.[159]

---

151. Dirk A. Zetzsche et al., *The Evolution and Future of Data Driven Finance in the EU*, 57 COMMON MKT. L. REV. 351 (2020).

152. GEVA, *supra* note 139, at 3. *See also* Benjamin Geva, *The Clearing House Arrangement*, 19 CAN. BUS. L. J. 138, 138 (1991); ROY GOODE, COMMERCIAL LAW 465 (3rd ed. 2004).

153. Hal S. Scott, *The Importance of the Retail Payment System* 5 (Retail Payment Systems Conference, Harv. L. School Program on Int'l Fin. Sys., Feb. 26, 2015).

154. MARK MANNING, ERLEND NIER & JOCHEN SCHANZ, THE ECONOMICS OF LARGE-VALUE PAYMENTS AND SETTLEMENT: THEORY AND POLICY ISSUES FOR CENTRAL BANKS 175 (2009). *See also* Georg, *supra* note 136, at 2220.

155. Kimmo Soramäki et al., *The Topology of Interbank Payment Flows*, 379(1) PHYSICA A: STATISTICAL MECHANICS & ITS APPLICATIONS 317, 318 (2007).

156. "The linkage among deposit taking, lending, and the provision of payment services, leading to the architecture of the modern payment system, is economically rationalized by the quest for efficiency gains." GEVA, *supra* note 139, at 8.

157. "[I]n an economy with many banks, it is inefficient for every agent to have an account with each other." MILLARD, HALDANE & SAPORTA, *supra* note 122, at 16. *See also* GEVA, *supra* note 139, at 9.

158. JOHN ARMOUR ET AL., PRINCIPLES OF FINANCIAL REGULATION 394 (2016).

159. MILLARD, HALDANE & SAPORTA, *supra* note 122, at 4.

However, as in open banking, the requirements to participate directly in banking payment systems can be prohibitive for some entities. The investment required in "hardware, software and procedures" as well as risk management measures means that flexibility in allowing indirect participation "can be more efficient, allowing greater competition among payment intermediaries in the provision of payment services to third parties" and enable participation by institutions who cannot directly participate.[160] Despite this, banking payment systems can also develop to be inefficient, resulting in poor use of financial resources and inequitable risk sharing.[161] These inefficiencies can develop from economies of scale and network externalities which can cause monopolistic practices and restrictions on fair access, participation and use, which can be "inherent in payment services."[162]

From this perspective, banking payment systems and open banking systems are functionally similar multilateral communication networks. Both systems benefit from multilateral participation and in both systems competitive market conditions "offer the most promising results in terms of efficiency and innovation."[163]

2. Stability

In banking payment systems, the "other side of the coin" to the benefits delivered by multilateral participation is the risk that the complex systems which result from the interconnectedness causes the failure of one participant to result in the failure of others. This complexity can be seen in Fedwire in the United States of America,[164] and in the "massive concentrations of financial technology under the control of individual

160. BANK FOR INT'L SETTLEMENTS, COMM. ON PAYMENT & SETTLEMENT SYS., *supra* note 121, at 36.

161. *Id*. at 7. *See also* RHYS BOLLEN, THE LAW AND REGULATION OF PAYMENT SERVICES: A COMPARATIVE STUDY 132 (2012).

162. Biagio Bossone & Massimo Cirasino, *The Oversight of the Payments Systems: A Framework for the Development And Governance of Payment Systems In Emerging Economies*, 12 WORLD BANK RSCH. SERIES, July 2001.

163. *Id*. at 16.

164. *See* Soramäki et al., *supra* note 155, at 317. *See also* Kimmo Soramäki et al., *Network Relationships and Network Models in Payment Systems: Bank of Finland Presentation*, BANK OF FIN., Aug. 24, 2005. Due to the limited number of settlement banks in the CHAPS payment system in the U.K., it is not scale-free and instead forms "a near-complete, well-connected, network": Christopher Becher, Stephen Millard & Kimmo Soramaki, *The Network Topology of CHAPS Sterling* 24 (Bank of Eng. Working Paper No. 355, 2008).

firms."[165] These complex interconnected systems can be both robust and fragile:[166]

> Just as electricity is delivered through a network for which the failure of a single power station can be disastrous, the vast majority of modern money is provided and operated by a network of banks in which the failure of one can disrupt the system as a whole'.[167]

This risk is known as systemic risk,[168] and it can be tremendously significant if it occurs in a banking payment system.[169] Banking payment systems "are the source of both remarkable economic prosperity and spectacular collapses,"[170] and over this time an understanding of the efficiency and risk in these systems has developed, together with the role that legal rights, responsibilities and relationships perform in their management,[171] and in their resilience.[172] Its management in the design of a system is critical because systemic risks cannot be efficiently managed by participants acting on their own, as the costs of a participant's failure are imposed beyond the transacting parties,[173] and it can arise from the "design and operation" of payment systems themselves.[174] Of particular importance in managing this risk in payment systems are rules and procedures which "limit the potential for the effects of a participant's failure to spread to other participants."[175] For these

---

165. Dirk A. Zetzsche et al., *Digital Finance Platforms: Towards a New Regulatory Paradigm*, 23(1) UNIV. OF PENN. J. BUS. L. 273 (2020).

166. Caldarelli & Catanzaro, *supra* note 121, at 97. "They are able to function normally even when a large fraction of the network is damaged, but suddenly certain small failures, or targeted attacks, bring them down completely." "Highly connected nodes seem to play a crucial role, in both errors and attacks."

167. FELIX MARTIN, MONEY: THE UNAUTHORISED BIOGRAPHY FROM COINAGE TO CRYPTOCURRENCIES 435 (2015).

168. *Supra* BANK FOR INT'L SETTLEMENTS, COMM. ON PAYMENT AND SETTLEMENT SYS. & INT'L ORG. OF SEC. COMMS., PRINCIPLES FOR FINANCIAL MARKETS INFRASTRUCTURES (Apr. 2012).

169. "We'd always thought that if you wanted to cripple the US economy, you'd take out the payment systems. Banks would be forced to fall back on inefficient physical transfers of money. Businesses would resort to barter and IOUs; the level of economic activity across the country could drop like a rock": ALAN GREENSPAN, THE AGE OF TURBULENCE: ADVENTURES IN A NEW WORLD 2 (2008).

170. ARMOUR ET AL., *supra* note 158, at 275.

171. *See* MANNING, NIER & SCHANZ, *supra* note 154, at ch. 1.

172. *See* Bossone & Cirasino, *supra* note 162, at 8.

173. Charles Kahn, Stephen Quinn & Will Roberds, *Central Banks and Payment Systems: The Evolving Trade-Off Between Cost and Risk* (Norges Bank Conference on the Uses of Central Banks: Lessons from History, June 5–6, 2014). *See also* Bossone & Cirasino, *supra* note 162, at 11.

174. MANNING, NIER & SCHANZ, *supra* note 154, at 35.

175. BANK FOR INT'L SETTLEMENTS, COMM. ON PAYMENT AND SETTLEMENT SYS. & INT'L ORG. OF SEC. COMMS, *supra* note 168, at 78.

reasons, as economies have become more dependent on the stability of payment systems, central banks and banking regulators have developed international standards to identify and manage this risk and components of it.[176] The most recent of these is the Principles for Financial Market Infrastructures (PFMIs).[177] The primary public policy objectives of these PFMIs is to "enhance safety and efficiency in payment, clearing, settlement, and recording arrangements, and more broadly, to limit systemic risk and foster transparency and financial stability."[178]

Trust and confidence is also a core component of stability in banking payment systems:[179] "a well-functioning financial system requires both confidence in the system and trust in the particular agents on whom stakeholders directly interact and rely."[180] In banking, this can be seen in the consequences of the loss of confidence leading to panic in a bank run, where "depositors rush to withdraw their deposits because they expect the bank to fail,"[181] and the collapse of Lehman Brothers in the global financial crisis which eroded "trust in the institutions—systemic trust—and the validity of the underlying principles."[182]

C. *Summary*

This Part shows that banking payment systems are networks for the transfer of valuable information and are functionally similar to open banking systems. Indeed, the economic description of a payment system as "any organized arrangement for transferring value between parties,"[183] would include open banking systems on the basis that data being transferred is valuable. This linkage between payment systems and communication or information systems is not new and "each is essentially

176. These standards contributed to stability during the 2008 global financial crisis. Daniela Russo, *CPSS-IOSCO Principles for Financial Market Infrastructures: Vectors of International Convergence*, 17 FIN. STABILITY REV. 69 (2013). *See also* Bossone & Cirasino, *supra* note 162, at 8.

177. BANK FOR INT'L SETTLEMENTS, COMM. ON PAYMENT AND SETTLEMENT SYS. & INT'L ORG. OF SEC. COMMS, *supra* note 168. *See also* BRINDLE & COX, *supra* note 144, at ¶ 1-026.

178. BANK FOR INT'L SETTLEMENTS, COMM. ON PAYMENT AND SETTLEMENT SYS. & INT'L ORG. OF SEC. COMMS, *supra* note 168, at ¶ 1.15.

179. "The core of payments and money is therefore trust or, rather, lack of trust in each other's creditworthiness—we don't trust each other but we do trust the system." LEIBBRANDT & DE TERAN, *supra* note 101, at 17.

180. *Id*. at 180.

181. *See* Douglas W. Diamond & Philip H. Dybvig, *Bank Runs, Deposit Insurance, and Liquidity*, 24(1) FED. RSRV. BANK OF MINN. Q. REV. 14 (2000).

182. Roth, *supra* note 130. *See also* Earle, *supra* note 134. "[O]nce eroded, the system rapidly ground to a halt—money literally stopped moving." Gillespie & Hurley, *supra* note 128, at 180.

183. MANNING, NIER & SCHANZ, *supra* note 154, at 3. Legally, the description can be narrower, for example as the transfer of "monetary value." GEVA, *supra* note 142, at 2.

a different branch of the same network family tree."[184] Further, the focus on safety and efficiency in payment systems "owes much to the understanding that sound network infrastructures in crucial domains such as communications, information and financial transactions are essential to sustain the international competitiveness of the domestic economy."[185]

The functional similarity between open banking systems and banking payment systems enables the evaluation of the legal features of the Australian and U.K. open banking systems governing access and stability in participation against those which do so in banking payment systems. This analysis is contained in Parts IV and V of this Article. Before this, Part III explains the choice of the open banking systems of those jurisdictions for this analysis.

III. RELEVANCE OF OPEN BANKING IN AUSTRALIA AND THE U.K. TO THE U.S.

The access and stability features of open banking laws in Australia and the U.K. are highly relevant for the legal design of open banking in America for several reasons. First, like the aim in the U.S., the rights of customers to share their data in Australia and the U.K. are contained in legislation, rather than being the result of the voluntary adoption of technological standards by banks.[186] Accordingly, substantive legal analysis can be conducted on the open banking systems of Australia and the U.K..[187] Second, Australia and the U.K. are the two leading common law jurisdictions in establishing a legislative basis for open banking. The legal foundations for open banking were established in the U.K. in 2017,[188] and in Australia in 2019.[189] Third, the primary objectives for implementing open banking in both jurisdictions were similar to those

184. Andrew G. Haldane, *Rethinking the Financial Network*, *in* FRAGILE STABILITÄT–STABILE FRAGILITÄT 243, 244 (Stephan A. Jansen, Eckhard Schröter & Nico Stehr eds. 2013).

185. Bossone & Cirasino, *supra* note 162, at 14.

186. These can be described as "regulatory" frameworks or "mandatory" frameworks. In other jurisdictions, such as Singapore and Hong Kong, there is no legal obligation to participate, even though government authorities are involved in setting the standards under which participation occurs. These can be described as "voluntary" frameworks. The BIS uses different characterization, being "prescriptive approach," "facilitative approach" and "market-drive approach": BANK FOR INT'L SETTLEMENTS, *supra* note 10. This mixes legal obligation with standardization and includes consideration of the intention of authorities in the characterization.

187. The same analysis cannot be conducted on voluntary frameworks which are not supported by laws and regulations as they do not provide a consistent legal framework for all bank customers to share their data. CGAP (Consultative Group to Assist the Poor), housed and administered by the World Bank, considers that a regulatory mandate or other regulatory support is required for an arrangement to constitute open banking: Plaitakis & Staschen, *supra* note 84.

188. COMPETITION & MKTS AUTH., *supra* note 10.

189. COMMONWEALTH TREASURY, *supra* note 91, at 3. The author led this inquiry.

expressed in America: to improve competition,[190] encourage innovation,[191] and enhance consumer protection.[192] Fourth, despite these similarities the legal foundations of open banking in Australia and in the U.K. are significantly different so that insights can be drawn for open banking design in the U.S. from the different approaches taken. These differences are introduced next.

A. *The Legal Foundation for Open Banking in Australia*

Open banking in Australia is the first stage of the Consumer Data Right (CDR), an economy-wide right designed to enable consumers to obtain value from the use of their data.[193] It was established under the *Treasury Laws (Consumer Data Right) Act 2019* (*CDR Act*),[194] which created the CDR in a new Part IV.D of the *Competition and Consumer Act 2010* (*CCA*).[195] The CDR can apply to sectors of the Australian economy by designation of the Australian Treasurer through legislative instrument,[196] and the *Consumer Data Right (Authorised Deposit Taking Institutions) Designation 2019* (*Open Banking Designation*)[197] made such a designation for the banking sector. The *CCA* and the *Open Banking Designation* are complemented by the *Competition and Consumer (Consumer Data Right) Rules 2020* (*CDR Rules*) issued by the Australian Competition and Consumer Commission (ACCC), and the standards (Australian Standards) for "the format and description of CDR data" and "the disclosure of CDR data" issued by the Data Standards Chair.[198]

1. The Legal Foundation for Open Banking in the U.K.

In contrast, two separate legislative instruments form the legal foundation of U.K. open banking: Part 2 of the Retail Banking Market

190. For the U.K., *see* COMPETITION & MKTS. AUTH., *supra* note 79, at ⁋ 13.6; Fin. Conduct Auth., *supra* note 54, at ⁋ 1.4. *See also* Colangelo & Borgogno, *supra* note 26. For Australia, see Scott Morrison, TREASURY, *supra* note 56; COMMONWEALTH TREASURY, REVIEW INTO OPEN BANKING: GIVING CUSTOMERS CHOICE, CONVENIENCE AND CONFIDENCE (Dec. 2017). The author led this review.

191. For the U.K., *see* HM Treasury, *supra* note 75. For Australia, *see* Commonwealth Treasury, *supra* note 76.

192. *See* McKee, Whitaker & Millar, *supra* note 69, at 86. *See also* Vezzoso, *supra* note 95, at 34. *See also* Commonwealth Treasury, *supra* note 76, at 5.

193. PRODUCTIVITY COMM. (AUSTL.), *supra* note 150.

194. *Treasury Laws Amendment (Consumer Data Right) Act 2019* (Cth.) (Austl.).

195. *Competition and Consumer Act 2010* (Cth.) (Austl.).

196. *Id*. s. 56AC.

197. *Consumer Data Right (Authorised Deposit Taking Institutions) Designation 2019* (Cth.) (Austl.).

198. *Competition and Consumer Act 2010* (Cth.) s. 56FA (Austl.).

Investigation Order 2017 (U.K.) (CMA Order)[199] of the CMA, and Part 7 of the Payment Services Regulation 2017 (U.K.) (PSR).[200] The CMA Order was made to address a competition problem in the retail banking market identified by the U.K. Competition and Markets Authority (CMA),[201] whilst the PSR translated the EU's Revised Payment Services Directive (PSD2)[202] into U.K. legislation.[203] However, the CMA Order provides only a very limited outline of the legal requirements for open banking although it required that the OBIE be established to create data standards (U.K. Standards)[204] for the sharing of data under U.K. open banking. The PSR expresses the more detailed legal requirements. It also requires compliance with an EU Regulatory Technical Standard relating to Strong Customer Authentication (SCA-RTS),[205] which provides the basis on which the U.K. Standards are approved for compliance with the PSR for a U.K. bank.[206]

This difference in legal foundation of open banking between Australia and the U.K. stands in contrast with the close connection and similarity in their banking laws, and the regulatory principles related to their banking payment systems.[207] Much of banking law in Australia and the U.K. is based on the common law of contract and agency, which differ little between the two jurisdictions as they have a shared legal heritage.[208] Also each jurisdiction adheres to the PFMIs.[209] This similarity, when combined with the similarity in the objectives of open banking and the reliance on broad and diverse participation to achieve them, enables a meaningful analysis of the differences in the legal features which support

199. Retail Banking Market Investigation Order, 2017 (U.K.). The order is made under the Enterprise Act, 2002 (U.K.).

200. Payment Services Regulation, 2017 (U.K.).

201. COMPETITION & MKTS. AUTH., *supra* note 79, at 57. *See also* VICTORIA DIXON, GOODE ON PAYMENT OBLIGATIONS IN COMMERCIAL AND FINANCIAL TRANSACTIONS 189 (4th ed. 2020).

202. PSD2, *supra* note 74.

203. Explanatory Memorandum, Payment Services Regulation, 2017 (U.K.).

204. Retail Banking Market Investigation Order, 2017 (U.K.), art. 14.

205. Commission Delegated Regulation (EU) 2018/389 Supplementing Directive (EU) 2015/2366, of the European Parliament and of the Council, with regard to Regulatory Technical Standards tor Strong Customer Authentication and Common and Secure Open Standards of Communication, 2017 O.J. (L 69) 23 (hereinafter SCA-RTS). *See also* Payment Services Regulation, 2017 (U.K.) pt. 9, reg. 70(2)(a).

206. SCA-RTS, *supra* note 205, art. 30.

207. *See* PHILIP WOOD, COMPARATIVE FINANCIAL LAW 49 (1995).

208. The principal English cases which form the basis of the banker-customer relationship have been followed and approved by Australian courts: *see* cases cited *infra* note 141.

209. *See* Bank of Eng., *Financial Market Infrastructure Supervision* (June 14, 2022), https://www.bankofengland.co.U.K./financial-stability/financial-market-infrastructure-supervision [https://perma.cc/8J5H-3KZA]; Rsrv. Bank of Austl., *Implementing the CPSS-IOSCO Principles for financial market infrastructures in Australia* (Feb. 2013), https://www.rba.gov.au/payments-and-infrastructure/financial-market-infrastructure/principles/implementation-of-principles.html [https://perma.cc/3ZN8-BRQE].

access and stability of participation under open banking between the jurisdictions. Although the banking and payments law of the United States differs from that in Australia and the U.K., the objectives of open banking and the functions which achieve those objectives are similar. Accordingly, the analysis conducted in the next Parts of this Article is very relevant to the design of open banking in the U.S.

IV. ENABLING ACCESS TO PARTICIPATION IN OPEN BANKING SYSTEMS

Part I has shown that designing the legal governance of access to participation in open banking involves balancing a series of competing principles. For open banking to be effective in achieving its objectives, customer banking data must be shared with recipients who will use it.[210] Accordingly, it is important that *access* to open banking is provided to data recipients who will receive and use customer data as the customer requires, and the service providers who support them. This is fundamental to the data portability and customer autonomy functions of open banking described in Part I. However, trust in open banking rests on recipients of customer data being accountable for the protection and use of shared customer data and to provide confidence that the recipient accountability function of open banking can be performed. Open banking systems commonly require that those who directly participate by receiving shared customer data be accredited or authorized. As noted in Part II, achieving this authorization can be beyond the reach of smaller entities so enabling access for them requires facilitation of indirect participation. Also, many of those who choose to participate (either directly or indirectly) retain and rely on intermediaries and third parties who provide technological and other support services. Accordingly, the authorization needed to participate directly, the requirements for indirect participation, and the conditions on outsourcing are all important for enabling access to open banking for those involved in the collection, storage and use of customer data. The legal requirements for these under Australian and U.K. open banking are comparatively analyzed below, in each case followed by evaluation against the equivalent principles in the regulation of access to banking payment systems.

210. Although customer data is regarded as being valuable, the value arises from customer data "because of its usefulness." FLORIDI, *supra* note 113, at 90. Or "what can be done to create value" with the data. Peter Leonard, *The Good Oil on Valuing 'The New Oil'* (2018) 24(7) COMPUT. & TELECOMM. L. REV. 167. *See also* Martens, *supra* note 39. This usefulness is facilitated by the structuring of the data to be shared through the use of common standards, so that the data have significant semantic character, or meaning, when they are received: *see* FLORIDI, *supra* note 113.

A. *Direct Participation*

1. Comparison of Authorization to be a Data Recipient in Open Banking

Authorization to receive data under Australian open banking is granted as part of the regulation of Australia's CDR. The legal foundations of the CDR are set out in Part III above. In this legislative context, an accredited data recipient (ADR) is a person accredited by the ACCC,[211] and who has received customer data (which is more precisely defined as "CDR data")[212] under the *CDR Rules*.[213] Requirements for accreditation of data recipients known as Accredited Data Recipients of ADRs are set out in the *CDR Rules*,[214] including information security,[215] customer compensation, and dispute resolution process requirements, and "fit and proper person criteria."[216] Whilst *CCA* requires that the 'Data Standards Chair' creates standards for the format and description of shared data and the disclosure of shared data,[217] those are not directly relevant to the authorization of data recipients.[218]

In U.K. open banking, the *CMA Order* requires that the U.K. standards to include provisions relating to "whitelisting as a system for approving third party providers fairly and quickly unless there is sufficient existing regulatory oversight."[219] Those regulatory requirements are provided by the PSR which requires that data be shared by account servicing payment service providers (ASPSPs) with account information service providers (AISPs).[220] AISPs are required to register with the Financial Conduct

---

211. The ACCC is the *Data Recipient Accreditor: Competition and Consumer Act 2010* (Cth.) ss. 56CA, 4(1) (Austl.) (definition of "Data Recipient Accreditor").

212. See Farrell, *supra* note 40, for further details on CDR data.

213. *Competition and Consumer (Consumer Data Right) Rules 2020* (Cth.) r. 5.12 (Austl.) [hereinafter CDR Rules]. *See also Competition and Consumer Act 2010* (Cth.) s. 56AK (Austl.).

214. *Competition and Consumer Act 2010* (Cth.) ss. 56BB(d), 56BH (Austl.).

215. *Competition and Consumer Act 2010* (Cth.) s. 56EO (Austl.) (In order to be accredited, a data recipient must take prescribed steps to protect customer data from misuse, interference and loss, unauthorized access, modification and disclosure). CDR Rules, *supra* note 213, r. 5.12(a) (This obligation is repeated in the *CDR Rules*). CDR Rules, *supra* note 213, r. 7.11, sch. 2 (The steps are operational in nature: to define and implement security governance, define the boundaries of the customer data environment, have and maintain an information security capability, implement a formal controls assessment program and have plans to manage and report security incidents). CDR Rules, *supra* note 213, r. 7.11, sch. 2 (The *CDR Rules* also require there to be Australian Standards about the security of customer data).

216. CDR Rules, *supra* note 213, r. 5.12.

217. *Competition and Consumer Act 2010* (Cth) s. 56FA (Austl.).

218. Other than in relation to information security requirements.

219. Retail Banking Market Investigation Order, 2017 (U.K.), ¶ 10.2.3.

220. Payment Services Regulation, 2017 (U.K.), reg. 70.

Authority (FCA) unless they already hold a broader authorization under the PSR.[221]

The requirements for registration as an AISP include those relating to information security,[222] customer compensation, security-related customer complaints,[223] and good repute and payments experience of directors and managers.[224]

Despite the material difference in legislative foundations, in broad terms the eligibility requirements for ADRs under Australian open banking and AISPs under U.K. open banking are similar, with each having requirements directed at good standing, access to dispute resolution processes, information security,[225] and customer compensation arrangements.[226] Further, there are similar technological requirements to be satisfied in order to have operational access.[227] However, there is an important conceptual difference in the nature of the authorizations.

Although accreditation under Australian open banking authorizes an ADR to request, receive, and use shared data, it does not authorize any particular service to be provided by the ADR using the data. If an ADR uses shared data to provide a service which is subject to regulation beyond Part IV.D of the *CCA*, then the ADR will need to obtain the authorizations required by that other regulation. For example, an ADR

---

221. *Id*. reg. 2(1); *id*. reg 14(4) (definitions of "payment service" and "payment service provider." Other than an authorization under PSR as a small payment institution).

222. AISPs must have a security policy and procedure for monitoring, handling and following up security incidents: *id*. reg. 17, sch 2. The PSR also requires an AISP to establish a risk management framework for operational and security risks: *id*. reg 98(1). An AISP is also required to notify the FCA of any major security incident, and its customers if it has, or may have, an impact on their financial interests: *id*, reg 98. In addition, The *CMA Order* requires that the U.K. Standards include security standards: Retail Banking Market Investigation Order 2017 (U.K.), ¶ 10.2.3.

223. Payment Services Regulation 2017 (U.K.), reg. 17, sch. 2. Dispute resolution processes are also dealt with in regulation 101 of the PSR.

224. *Id*. reg. 17, sch 2.

225. Without going into the technical detail of the requirements, each framework requires data recipients to adhere to a security profile based on similar technical foundations and the breadth of coverage under each framework is similar in that each addresses the broad information security concepts of confidentiality (preventing unauthorized disclosure), integrity (preventing unauthorized modification) and availability (ensuring that information is available to be processed and transmitted).

226. There are some subtle differences in the insurance required; for a further explanation, see Farrell, *supra* note 45.

227. *See generally* Austl. Competition & Consumer Comm., *Participant On-boarding Guide* (June 2021), https://www.cdr.gov.au/sites/default/files/2021-07/CDR_Participant%20On-boarding%20Guide_v1.3_6.pdf [https://perma.cc/CN4T-KQD7] (laying out the requirements for enrollment to have operation access); Open Banking Implementation Entity, *Enrolling onto the OBIE Directory* (Nov. 2020), https://www.openbanking.org.U.K./wp-content/uploads/Enrolling-Onto-Open-Banking-Guide.pdf [https://perma.cc/3M3E-SQSM] (additional details regarding the requirements for enrollment to have operation access).

that uses the shared data to provide a financial service regulated by the *Corporations Act 2001* (*Corporations Act*), such as the provision of financial product advice,[228] is also required to obtain the license required under the *Corporations Act* to provide that advice.[229] In contrast, nothing other than authorization as an AISP is required under U.K. open banking to request, receive and use shared data "to provide consolidated information on one or more payment accounts held by the payment service user with another payment service provider or with more than one payment service provider,"[230] which is defined as an account information service.

Accordingly, authorization to participate as an ADR in Australian open banking is a necessary, but may not be a sufficient, condition to provide a service using shared customer data, whilst authorization to participate as an AISP in U.K. open banking is necessary *and* sufficient to provide the account information service using shared data. The conceptual difference between the authorization frameworks can also be seen in the different regulators which authorize participation, being an economy-wide competition regulator in Australia and the regulator of payment services in the U.K. It can also be seen in the different good standing requirements, which relate to the performance of payment services in the U.K.[231] and relating to sharing information "safely, efficiently and conveniently" in Australia.[232]

It could be argued that the simplicity and efficiency provided by the requirement for only a single authorization in U.K. open banking assists in encouraging participation and access, whereas the potential need for multiple authorizations in Australian open banking depending on the use to which the data is put could have the opposite effect. However, it is important to understand the limits of the authorization to participate in U.K. open banking as an AISP. It permits only the provision of an account information service, and no other authorizations are available under the PSR to permit the use of the shared data to provide other services (other than to initiate payments).[233] The provision of a similarly limited service

228. *See Corporations Act 2001* (Cth) s 766B (Austl.).

229. The license required for carrying on a business of providing financial services in Australia is an Australian Financial Services License. *Id*. at s 911A.

230. Payment Services Regulation 2017 (U.K.), reg. 2(1) (definition of "account information service").

231. *Id*., reg. 17, sch. 2.

232. Austl. Competition & Consumer Comm., *Accreditation Guidelines*, 10 (Dec. 9, 2020). If a data recipient under the Australian framework provided a regulated financial service, then in order to obtain the requisite Australian Financial Services License, they would need to demonstrate similar knowledge and experience to that required under the U.K. framework. *Corporations Act 2001* (Cth.) s 912A(1) (Austl.),.

233. There is a separate authorization for payment initiation services. *See* Payment Services Regulation 2017, SI 2014/421, art. 1, ¶ 2 (U.K.) (defining payment initiation service).

should not require a further authorization in Australia under either Australian financial service licensing requirements,[234] or Australian credit licensing requirements.[235] Accordingly, this difference should not result in greater access or participation under U.K. open banking than under Australian open banking. It could also be argued that the additional flexibility provided by not constraining an ADR to providing a single service using the shared data assists in encouraging access to Australian open banking whereas this limitation could discourage some participation in U.K. open banking. However, this considers direct participation only, and does not consider the opportunities for indirect participation in the U.K. system, which is analyzed in the next Section below.

Nevertheless, this conceptual difference remains material for two reasons. First, it shows that U.K. open banking is regulated as part of the regulation of payment services, whilst Australian regulation treats it as its own system for communicating data. Second, as a conceptual matter, the authorization to directly participate by receiving customer data under Australian open banking only provides access to the communication network and the data shared through it, whilst authorization under U.K. open banking combines access to the network and permission to provide a single service using the shared data. This is meaningful when these different approaches are evaluated against the approaches taken to authorize direct participation in payment systems.

2. Evaluation Against Conditions to Access Payment Systems

Direct participation in banking payment systems in both Australia and the U.K. is governed by their conditions for access.[236] A key function performed by these conditions is to manage the systemic risk which could be caused by the failure of a participant to perform its obligations due to the interconnectedness created by the system described in Part I.C.2 above. Therefore, conditions are imposed on access to payment systems by limiting participation to those entities which are less likely to cause

234. Unless it is financial product advice, by being a "recommendation or a statement of opinion, or a report of either of those things" which "is intended to influence a person or persons in making a decision about a particular financial product or class of financial products, or an interest in a particular financial product or class of financial products, or could reasonably be regarded as being intended to have such an influence." *Corporations Act 2001* (Cth.) s 766B (Austl.).

235. Unless it is credit assistance, by suggesting that a consumer apply for, remain in, or increase, a particular credit contract. *National Consumer Credit Protection Act 2009* (Cth) s 8 (Austl.) [hereinafter NCCP Act].

236. Such as the Reserve Bank Information and Transfer System (RITS) in Australia and Clearing House Automated Payment System (CHAPS) in the U.K.. *RITS Regulations 2022* (Cth.) s 2.1 (Austl.); *CHAPS Reference Manual, BANK OF ENGLAND* 9 2022, https://www.bankofengland.co.U.K./-/media/boe/files/payments/chaps/chaps-reference-manual.pdf [https://perma.cc/5CP4-B V9T].

systemic risk,[237] "to protect systems and their participants from participation in the system by institutions that would expose them to excessive legal, financial or operational risks,"[238] or to ensure that participants who share risks have similar prudential standing to absorb those risks.[239] Historically, there has been a preference to use authorization as a bank as a requirement for permission to participate in important payment systems.[240] In fact, analyses of payment systems "often take for granted that the institutional structure of these systems is deeply intertwined with the conventional banking system."[241] However, the use of authorization to take customer deposits as a condition for access to payment systems conflates the functions of storage and liquidity which can be performed with respect to customer funds.[242] Also, limiting access to payment systems causes competition concerns arising out of the protected market position of those participants who control access.[243] For this reason, "[i]t is generally accepted that competition authorities and regulators should try to minimize barriers to entry or exit."[244] As a result, international standards now prefer that the requirements "be justified in terms of safety and efficiency" and "be tailored to and commensurate . . . with . . . specific risks"[245] and "have the least restrictive impact on competition that circumstances permit."[246] This can be seen from the changes made to permit electronic money institutions and payment institutions authorized under the PSR to seek direct access membership of the primary interbank payment systems of the U.K..[247]

---

237. *See* MANNING, NIER & SCHANZ, *supra* note 154, at 59.

238. *Comm. on Payment and Settlement Sys.*, *supra* note 121, at ⁋⁋ 2.1, 3.9.1.

239. *Comm. on Payment and Settlement Sys.*, *General Guidance for National Payment System Development, BANK FOR INTERNATIONAL SETTLEMENTS* 34 (2006), https://www.bis.org/cpmi/publ/d70.pdf [https://perma.cc/C3S7-WKZA].

240. "Limiting membership to entities with high financial standing clearly increases the resilience of the system, as it reduces the probability that the net will be unwound due to member default. For instance, direct membership might be restricted to entities subject to close prudential supervision." MANNING, NIER & SCHANZ, *supra* note 154, at ⁋ 3.2.3.

241. Awrey, *supra* note 140, at 815.

242. *See id*.

243. "[A]ny limitation to free access creates rents and, hence, protected positions." Bossone & Cirasino, *supra* note 162, at 25.

244. Org. for Econ. Co-operation & Development, *Competition and Payment Systems* 6 (Roundtable Proceedings No DAF/COMP/(2012)24, 2012).

245. BANK FOR INT'L SETTLEMENTS, COMM. ON PAYMENT AND SETTLEMENT SYS. & INT'L ORG. OF SEC. COMMS, *supra* note 168, at 101.

246. BANK FOR INT'L SETTLEMENTS, COMM. ON PAYMENT AND SETTLEMENT SYS, *supra* note 121, at ⁋ 7.9.6.

247. CHAPS, Faster Payments, Bacs and Image Clearing System: *see* Bank of Eng., *Financial Conduct Authority and Pay.U.K., Access to U.K. Payment Schemes for Non-Bank Payment Service Providers* (Information Paper, Dec. 2019). The position in Australian interbank payment systems is not as advanced. For example, in addition to ADIs, only Australian licensed

This separation of the authorizations required to provide a financial service such as banking, and the conditions on admission to infrastructure which facilitates the performance of that service such as a payment system, is more aligned with the approach taken to accreditation of ADRs in Australia than the registration of AISPs in the U.K.. Australian open banking separates the authorization required to directly participate in the communication network to receive customer data from the authorization needed to provide services using the data shared. In doing so, the Australian system enables the requirements for specific risks to be managed, which can be different for sharing customer data and the services provided with them. In contrast, U.K. open banking uses the authorization required for the service provided using the shared data as the basis for participation in the communication network used for receiving it. This does not permit the tailoring of the requirements to the risks to be managed from different services and, as a result, U.K. open banking limits the services which can be provided by an AISP. This is akin to the historical approach of using authorization as a bank as the condition for admission to payment systems. Due to the limited requirements for registration as an AISP, the impact is not a reduction in the availability of access to U.K. open banking, as it is when authorization as a bank is used as a condition for direct participation in payment systems. Instead, due to the limited nature of the authorized services, there is a reduction in the breadth of the access which authorization enables. This difference results in U.K. open banking offering more restricted access to customer data than both Australian open banking and payment system regulation in relation to customer funds. However, this is balanced by the flexibility provided in indirect means of enabling participation in U.K. open banking.

B. *Indirect Participation*

1. Comparison of Indirect Participation in Open Banking

Initially, there were few options for indirect participation in Australian open banking. However, two years after its commencement, the Australian Government found that "current barriers to enter the CDR

central counterparties or securities settlement facilities and other institutions that are "an actual or prospective provider of third-party (customer) payment services with a need to settle clearing obligations" are able to hold an exchange settlement account allowing for direct settlement in the Reserve Bank Information and Transfer System (RITS): Rsrv. Bank of Austl., *Exchange Settlement Account Policy*, RSRV. BANK OF AUSTL., https://www.rba.gov.au/payments-and-infrastructure/esa/ [https://perma.cc/9VXD-SUSU]. However, the position is changing in Australia, *see* Australia, COMMONWEALTH TREASURY, PAYMENT SYS. REV.: FROM SYS. TO ECOSYSTEM (June 2021); Commonwealth Treasury, *Transforming Australia's Payments System* (Government Response, Dec. 2021). The author led the Payment System Review for the Commonwealth Treasury.

(including the cost of accreditation) are deterring many businesses from participating."[248] Amendments were made to the *CDR Rules* to address this deficiency and to "facilitate greater participation in the CDR regime by participants and consumers, provide greater control and choice to consumers in sharing their data; promote innovation of CDR offerings including intermediary services, and enable services to be more effectively and efficiently provided to customers."[249]

The changes which most affected indirect participation were the introduction of a "sponsored" level of accreditation and the ability for a data recipient with unrestricted accreditation to appoint representatives.

Different levels of accreditation were always contemplated in Australian open banking "to reflect the different risks associated with different data sets and data uses."[250] Accordingly, the *CCA* specifically provides for different levels corresponding to the different risks of specified classes of customer data, specified classes of activities and specified classes of applicants for accreditation.[251] Despite this, the *CDR Rules* originally only provided for an "unrestricted" level of accreditation,[252] until they were amended to permit a data recipient to seek accreditation at a new "sponsored" level if they have arrangements with another data recipient (a sponsor) which has an unrestricted level of accreditation, including a written sponsorship agreement with the sponsor as well as assistance and training on technical and compliance matters from the sponsor.[253] Under sponsored accreditation, the sponsor is required to take reasonable steps to ensure that the sponsored participant complies with their obligations as an accredited person.[254] Consequently, the sponsored data recipient can become accredited in a less costly manner.[255] However, the sponsored data recipient may only make requests for customer data through their sponsor and may not make requests directly to a customer.[256] The result is that a sponsored participant could provide account information service if it were: (1) sponsored by a bank; (2) participate in a digital marketplace using customer data if it were sponsored by the marketplace operator; (3) use

248. CDR Rules Version 3 EM, *supra* note 110, at 3.

249. *Id*. at 1.

250. Commonwealth Treasury, *supra* note 76, at 8.

251. Competition and Consumer Act 2010 (Cth) s. 56BH(1)(d) (Austl.).

252. Austl. Competition & Consumer Comm., *supra* note 232, at ⁋ 2.2.

253. CDR Rules, *supra* note 213, rr. 5.1A, 5.1B. *See also Competition and Consumer (Consumer Data Right) Amendment (2021 Measures No. 1) Rules 2021* – Exposure Draft 2021 (Cth) sch. 1 (Austl.) [hereinafter CDR Rules Version 3].

254. *See* CDR Rules, *supra* note 213, at 5.1B(8).

255. *Id.* at sch. 1 (The sponsored data recipient does not need to provide an independent third-party assurance report in relation to its information security requirements and instead it is required to provide a self-assessment and attestation).

256. *Id*. at 5.1B(8).

data provided in a "data enclave" by the sponsor; and (4) "white-label" the CDR infrastructure services which the sponsor provides.[257]

U.K. open banking does not contemplate different levels of authorisation to provide account information services.[258] There is only a single level of authorisation available to provide account information services, which is registration as an AISP.[259] However, the PSR provides a similar level of flexibility in participation in U.K. open banking through the use of agents acting on behalf of an AISP in the provision of their account information service.[260] Although initially the PSR did not cover the use of agents by an AISP, it was found that the resulting inability of the FCA to require registration or removal of agents "leaves a gap in the regulatory regime which could lead to consumer detriment" and agents are now required to be registered with the FCA.[261] The application for the agent's registration is not as extensive as that required to be registered as an AISP. The requirements are: (1) identification information; (2) evidence that directors and management are fit and proper persons;[262] and (3) a description of the services for which the agent is appointed.[263] The AISP must ensure that its agents inform its customers of the agency arrangement.[264] The AISP is responsible for anything done by its agent in providing account information services on its behalf and must take all reasonable steps to ensure that the PSR is complied with by the agent.[265]

---

257. *See* CDR Rules Version 3, *supra* note 253, at 7.

258. *Id*. at reg. 14(4); *see also supra* note 221, at reg. 2(1) (definitions of "payment service" and "payment service provider.") Other than an authorization under PSR as a small payment institution:

> The PSR contemplates that payment institutions which have different authorizations can provide account information services but the different levels of these authorizations represent the different payment services which the payment institution is authorized to provide, not different levels of authorization to provide the account information services: Payment Services Regulation, 2017 (U.K.), reg. 2 (definitions of "account information service provider", "payment service provider").

259. *Id.* at reg. 17.

260. *Id.* at reg. 2 (defintion of "agent"); *see also* Fin. Conduct Auth., *AISP Models under PSD2* (Guidance, 21 Jan. 2020), https://www.fca.org.U.K./firms/agency-models-under-psd2 [https://perma.cc/2HG7-37UX].

261. *See* Payment Services Regulation, 2017 (U.K.), reg. 34; *see also* The Payment Systems and Services and Electronic Money (Miscellaneous Amendments) Regulations, 2017 (U.K.), reg. 7; Explanatory Memorandum to the Payment Systems and Services and Electronic Money (Miscellaneous Amendments) Regulations, 2017 (U.K.) ¶ 7.7.

262. *See supra* note 221 (Where the agent is not itself a payment service provider under the PSR: FIN. CONDUCT AUTH., PAYMENT SERVICES AND ELECTRONIC MONEY: OUR APPROACH ¶ 5.18 (June 2019)).

263. *See* Payment Services Regulation, 2017 (U.K.), reg. 34(3).

264. *Id.* at reg. 34(16).

265. *Id.* at reg. 36.

For this purpose, the AISP is expected "to have appropriate systems and controls in place to oversee their agents' activities effectively."[266] An agent may be removed from the register by the FCA if the registration was obtained falsely, it is desirable in order to protect the interests of consumers or the agent's provision of service is unlawful.[267]

A function similar to that performed by agents of an AISP under U.K. open banking can now be performed by "representatives" of an ADR under Australian open banking. An ADR with unrestricted accreditation can appoint an unaccredited person as their representative to seek customer consent to receive data and to use the data shared so that the representative can provide goods or services to the customer.[268] There must be a written contract between the data recipient and the representative containing prescribed terms relating to the use and treatment of the data and the data recipient is legally required to ensure that the representative complies with that contract and is responsible for breaches of the *CDR Rules* by its representative.[269] The CDR representatives of a data recipient are required to be notified to the ACCC and disclosed to customers.[270]

The result of the ability of AISPs to appoint agents and for ADR's to sponsor other data recipients and appoint representatives is that access to open banking through indirect participation is broadly similar in Australia and the U.K.. In each jurisdiction an authorised entity is responsible for the actions of the indirect participant and requirements for binding arrangements between them.

The above analysis focusses on indirect participation from "within" the open banking system. U.K. open banking offers even more flexibility for indirect participation through the use of "third parties" or "another person" who can receive customer data without being subject to regulation under the PSR. This is permitted by the definition of "account information service" in the PSR, which allows for the consolidated information on the customer's payment accounts to be provided "to another person in accordance with the payment service user's instructions."[271] It enables an AISP to provide the information to another

266. FIN. CONDUCT AUTH., *supra* note 262, ¶ 5.3.

267. Payment Services Regulation, 2017 (U.K.), reg. 35(1).

268. The accredited data recipient makes the request for the shared data and shares the data received with the representative. CDR RULES, *supra* note 213, at r. 1.10AA.

269. Competition and Consumer (Consumer Data Right) Rules 2020 with propsoed amendments, Aus. Fed.Reg. of Leg. §§ 1.10AA, 1.10A, 1.16A, 4.3A – 4.3C, 7.3, 7.6, 7.8A, 7.10A, 7.11, 7.16.

270. *Id.* §§ 5.14, 7.2.

271. Payment Services Regulation, 2017 (U.K.), reg. 2 (definition of "account information service").

entity who is not regulated under the PSR, with the customer's consent,[272] and permits the use of the shared data beyond the provision of the account information service for which the AISP is authorised, for example "credit scoring, mortgage applications or loan applications" and the passing of that information to a loan company.[273] This use would not otherwise be permitted due to the limits on the services able to be offered by direct participation analysed in Part II.A above. However, these third parties involved in the collection, processing and use of customer data, which are not AISPs nor agents of them, are not subject to PSR,[274] but are subject to the U.K.'s implementation of the General Data Protection Regulation (GDPR)[275] with respect to that data.[276] This is not the same as the responsibilities imposed on AISPs for the agents which they appoint to act on their behalf. If it were, then there would have been no need to amend the PSR to include agents appointed by an AISP within the scope of FCA regulation.[277]

Australian open banking does not offer similar flexibility in sharing customer data beyond open banking. Whilst the *CDR Rules* also permit some disclosures of customer data to those outside its regulatory perimeter, these are limited to disclosures to specified classes of "trusted advisors"[278] who "as members of a professional class, . . . are subject to existing professional or regulatory oversight, including obligations consistent with safeguarding consumer data (e.g., fiduciary or other duties to act in the best interests of their clients)."[279] Although, like the use of third parties under U.K. open banking, this enables shared data to be provided to someone beyond Australian open banking's regulatory perimeter with the customer's consent. It limits this to recipients who

272. FIN. CONDUCT AUTH., *AISP Models under PSD2* (Jan. 21, 2020), https://www.fca.org.U.K./multimedia/aisp-models-under-psd2 [https://perma.cc/2HG7-37UX].

273. *Id.*

274. "More than one business may be involved in obtaining, processing and using payment account information to provide an online service to a customer. However, the business that requires authorization or registration to provide the account information service is the one that provides consolidated account information to the payment service user (including through an agent) in line with the payment service user's request to that business": FIN. CONDUCT AUTH., FCA HANDBOOK [PERG 15.3 Q25A] (2013).

275. GDPR, *supra* note 23. Following the withdrawal of the U.K. from the EU, *GDPR* effectively became part of the domestic law of the U.K. to create a "U.K. GDPR": European Withdrawal Act, 2018 (U.K.), s. 3; Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations, 2019 (U.K.). However, for simplicity this Article will refer to it as the GDPR.

276. FIN. CONDUCT AUTH., *supra* note 260.

277. *See supra* note 261 and accompanying text.

278. Including qualified accountants, practicing lawyers, registered tax agents and advisers, financial counseling agencies, regulated financial advisers and financial planners and mortgage brokers. CDR Rules, *supra* note 213, at 1.10C.

279. CDR Rules Version 3, *supra* note 253, at 15.

already owe professional duties to the customer, rather than merely being subject to generally applicable data protection legislation. The consequences of this difference are evaluated against indirect participation in payment systems next.

2. Evaluation Against Indirect Participation in Payment Systems

Indirect participation in a payment system arises when direct participants make payments in the system on behalf of others who are not direct participants.[280] This results in "tiering" of participation in the system,[281] which provides benefits by avoiding the expense of direct membership for the indirectly participating entities, providing economies of scale in processing and reducing liquidity demands through internalization of payments and liquidity pooling amongst the customer entities.[282] However, indirect participation can also increase the risk in the system, as the liquidity and credit risks of the customer entities are concentrated in the directly participating entity and the indirect participants take increased operational risk on the direct participant bank.[283] Also, the indirect participants create risks for the direct participant as the direct participant is responsible to the payment system for their performance. This is particularly material where the number and size of indirect transactions is large in comparison to those of direct participation.[284] To manage these risks, a payment systems rules are required to contain "procedures, rules, and agreements with direct participants allow it to gather basic information about indirect participants in order to identify, monitor, and manage any material risks to the FMI arising from such tiered participation arrangements."[285]

The sponsored level of accreditation and the ability to appoint representatives under Australian open banking, and the ability to appoint agents under U.K. open banking, are consistent with approach taken to regulation of indirect participation in payment systems. In each case the data recipient is responsible for the entity which it sponsors or which it has appointed as its representative or agent and the regulator is required to be notified of the sponsored recipient, representative or agent. However, this alignment with payment systems does not extend to the ability for an AISP to use third parties without any registration or

280. MANNING, NIER & SCHANZ, *supra* note 154, at 170.

281. *Id.* at 169. *See also* BANK FOR INT'L SETTLEMENTS, COMM. ON PAYMENT AND SETTLEMENT SYS. & INT'L ORG. OF SEC. COMMS, *supra* note 168, ¶ 3.19.1.

282. MANNING, NIER & SCHANZ, *supra* note 154, at 170. *See also* MILLARD, HALDANE & SAPORTA, *supra* note 122, at ch. 9.

283. MANNING, NIER & SCHANZ, *supra* note 154, ¶ 10.2.

284. BANK FOR INT'L SETTLEMENTS, COMM. ON PAYMENT AND SETTLEMENT SYS. & INT'L ORG. OF SEC. COMMS, *supra* note 168, ¶ 3.19.3.

285. *Id.* at 64.

notification requirements, or responsibility to the customer, under U.K. open banking. Payment systems do not customarily enable funds to be paid beyond the direct participants of the system. Instead, payments to those "beyond the system" are conducted through the accounts held with indirect participants and those who have banker-customer or other account relationships with the customer. This is more aligned with the recent changes to the *CDR Rules* which permit data to be shared outside of the CDR only with specified classes of regulated "rusted advisors." This ensures that there is still a regulated relationship between the recipient of the shared data and the customer which imposes duties in the customer's favor, beyond those under generally applicable law.

It could be argued that the ability for customers to consent to their data being shared with others beyond U.K. open banking is no different to the customer sharing the information themselves by some other process. Whilst this is true from the customer's perspective, from a systemic perspective this is different because of the impact of misuse of customer data on the credibility of the open banking system. If a customer suffers loss because of the misuse of their data which has been shared using open banking, and the open banking system provides no regulatory remedy because the data was shared with someone beyond its regulatory perimeter, then the trust in the system will be damaged. As the analysis in Part I.C shows, this loss of trust can affect the confidence in the open banking system as a whole, and its continued use by customers and participants. U.K. open banking relies on the GDPR to guard against that loss of trust. Australian open banking takes a more robust approach, not solely relying on Australia's privacy legislation, the *Privacy Act*,[286] but by ensuring that there is a regulated professional relationship with the customer protecting the use of the shared data. This difference means that U.K. open banking offers greater access to customer data than Australian open banking and that which payment system regulation offers in relation to customer funds. However, the trade-off for this is a reduction in the directness of accountability to the customer for the customers for the use and custody of customer data.

C. *Outsourcing Arrangements*

1. Comparison of Regulation of Outsourcing Arrangements in Open Banking

The *CDR Rules* offer further flexibility in access to customer data by enabling them to be disclosed under "CDR outsourcing arrangements."[287]

286. *Privacy Act 1988* (Cth) (Austl.).
287. CDR Rules, *supra* note 213, at 1.10.

These are written contracts between two persons under which one of them (the "provider") will either:

> collect customer data on behalf of the principal, or
>
> provide goods and services to the other person (the "principal") using the data.[288]

Under the contract, the provider must, at the principal's direction, provide the principal with access to the customer data, return or delete the data, and direct any person to whom it has disclosed the data to do the same.[289] The provider must take the same information security steps to protect any customer data collected by it, or disclosed to it, as part of the arrangement, or which derives from that data.[290] Also, the provider must not disclose that data to another person, unless the disclosure is under another CDR outsourcing arrangement.[291] The principal must, if it is an accredited person, ensure that the provider complies with its obligations,[292] and any use or disclosure of the customer data by the provider is taken to have been by the principal, whether or not the use or disclosure was in accordance with the outsourcing arrangement.[293] This prevents the customer data from being used or disclosed by the provider to another person, unless such disclosure would be permitted by the data recipient. In addition to these obligations, the accredited person must provide to customers a list of the outsourced service providers used, the nature of services provided by each of them, and the customer data that may be disclosed to each of them, as part of the accredited entity's CDR policy.[294] This approach to outsourcing is the result of changes made to the original design of the Australian system. Originally, outsourcing arrangements permitted the use of agents, but if the agent was not accredited at the unrestricted level, these only permitted goods or services to be provided to the data recipient. These constraints were recognized as a weakness in the access to Australian open banking and *CDR Rules* were amended to permit unaccredited outsourced service providers to collect customer data on behalf of an accredited entity.[295]

U.K. open banking is more flexible in the use of outsourced service providers. An AISP is able to use "technical service providers" which obtain and process customer information to support the AISP. Provided they do not have any direct relationship with the customer, technical

288. *Id.* at 1.10(2)(a).
289. *Id.* at 1.10(2)(b).
290. *Id.* at 1.10(2)(a), 1.10(2)(b)(i).
291. *Id*. at 1.10(2)(b).
292. *Id.* at 1.16.
293. *Id.* at 7.6(2).
294. *Id.* at 7.2(4).
295. CDR Rules Version 3, *supra* note 253, § 4.3(c)(1)(f).

service providers do not need to be authorised or registered by the FCA.[296] The AISP remains responsible for compliance with the PSR when a technical service provider is being used.[297] Complementing this are outsourcing arrangements with persons to perform operational functions for the AISP without accessing the customer's account on behalf of the AISP. These are required to be included in the description of the AISP's structural organisation as part of an application to register as an AISP,[298] and changes to them must not cause the AISP to cease meeting the conditions of their registration.[299] The AISP is responsible for the acts and omissions of someone to which its activities are outsourced in the same way as it is for its agent.[300] It is noteworthy that more detailed requirements are applicable under the PSR to the outsourcing by entities authorised as payment institutions, such as requirements for notification to the FCA, contracts with the outsourcing provider, and the arrangements must not impair the quality of the entity's internal control or the ability of the FCA to monitor compliance with the PSR.[301] However, these are not applicable to an entity which is only receiving customer data as an AISP and not dealing with customer funds.

The primary difference between Australian and U.K. open banking with respect to outsourced service providers is in the detail of the regulation applicable to them. As noted above, they are subject to regulation under Australian open banking regardless of their relationship with the customer, and that regulation imposes responsibility and supervision requirements similar to those which are imposed under the PSR on authorised payment institutions but not on outsourcing by AISPs. This difference is evaluated against the regulation of outsourcing in payment systems next.

2. Evaluation Against Regulation of Outsourcing in Payment Systems

Outsourcing in payment systems is recognized to have the potential to create operational risk known as "concentration risk," which can affect the stability of not only the participants, but also others that depend on them and the system as a whole.[302] Accordingly, the standards applicable to their regulation require "robust arrangements for the selection and

296. FIN. CONDUCT AUTH., PERIMITER GUIDANCE MANUAL, GUIDANCE ON THE SCOPE OF THE PAYMENT SERVICES REGULATIONS 2017 § 15.3 ¶ Q25A (Apr. 2021).

297. *Id.*

298. FIN. CONDUCT AUTH., *supra* note 262, ⁋ 3.171.

299. *Id.* ⁋ 4.58.

300. Payment Services Regulation 2017, SI 2017 No. 752, reg. 36 (U.K.).

301. *See id*. at part 3, reg. 25(2).

302. *See* MANNING, NIER & SCHANZ, *supra* note 154, at 181; Fin. Stability Board, *Regulatory and Supervisory Issues Relating to Outsourcing and Third-Party Relationships*, at 14 (Nov. 9, 2020). *See also* Int'l Org. of Sec. Comms., *Principles of Outsourcing*, Consultation Report No. CR01/2020 (May 2020); Zetzsche et al., *supra* note 165.

substitution of such providers, timely access to all necessary information, and the proper controls and monitoring tools" and that "[a] contractual relationship should be in place between the FMI and the critical service provider allowing the FMI and relevant authorities to have full access to necessary information."[303]

The impact of outsourcing in relation to payment systems can also be seen in the regulation of banks as direct participants of interbank payment systems. Banks are "increasingly using third parties to carry out activities that the [banks] themselves would normally have undertaken,"[304] to reduce costs, access new technology, permit a focus on the banks' core business, and take the benefit of economies of scale.[305] However, outsourcing also brings risks to banks, which can arise through failure to oversee the outsourced provider, poor service from the outsourced provider, misalignment of strategy and practices by the outsourced provider, failure of the outsourced provider to comply with the laws which apply to the bank, technology failures by the outsourced provider, fraud and default of the outsourced provider, impediments to access to information, and concentration risk on the outsourced provider.[306] As a result, in each of Australia and the U.K., banks are required to adhere to regulations on material outsourcing.[307] This is particularly relevant for outsourcing information technology functions as they can be provided in a standardized, rather than tailored, form on a large scale and in an automated manner.[308] Banks are not able to see all of the connections between their outsourced service providers and the other participants in a payment system or, as a result, all of the potential risks which could arise.[309] Accordingly, the relevant regulators need to supervise the participants' outsourcing arrangements "identifying and monitoring risk concentrations at individual service providers and assessing whether or not such concentrations could pose a risk to the stability of the financial system."[310] This is enabled by ensuring participants have comprehensive

303. BANK FOR INT'L SETTLEMENTS, COMM. ON PAYMENT AND SETTLEMENT SYS. & INT'L ORG. OF SEC. COMMS, *supra* note 168, at 99.

304. Bank for Int'l Settlements, Joint Forum Rep., *Outsourcing in Financial Services*, at 1 (Feb. 2005).

305. *Id*. at 6. *See also* Daniel Gozman & Leslie Willcocks, *The Emerging Cloud Dilemma: Balancing Innovation with Cross-Border Privacy and Outsourcing Regulations*, 97 J. BUS. RSCH. 235, 235 (2019).

306. *See* Bank for Int'l Settlements, *supra* note 304, at 11–12.

307. *See* Austl. Prudential Regul. Auth., *Prudential Standard CPS 231 Outsourcing* (2017); Bank of Eng., Prudential Regul. Auth., *Supervisory Statement SS2/21 Outsourcing and Third Party Risk Management* (2021).

308. *See* Euro. Banking Auth., *EBA Guidelines on Outsourcing Arrangements*, at 15, Final Report No. EBA/GL/2019/02 (Feb. 25, 2019).

309. *Id.* at 108.

310. *Id.* at 5.

enforceable agreements with material outsourcing providers and that they notify regulators of their material outsourcing arrangements.[311]

The regulatory requirements relating to outsourcing in U.K. open banking are not as extensive as those applicable in payment systems. Unlike in Australia, U.K. open banking does not require that a contract with particular provisions be in place with outsourced service providers, and it does not have a clear disclosure obligation in relation to the identity and role of outsourced service providers. Under the PSR, conditions of a nature similar to those required under Australian open banking are needed only if the outsourcing relates to the payment of money, rather than the transfer of data.[312] Accordingly, the ability to properly identify and assess the risk that any concentration of service providers for data recipients could present to the U.K. system as a whole is less than that in Australian open banking and in payment systems.[313]

The potential consequences of this are particularly relevant in the context of technology service providers to data recipients. The technology requirements for authorization to directly participate in the Australian and U.K. systems are extensive, particularly with respect to information security. Smaller fintech companies or smaller banks who do not have the resources to develop these capabilities themselves will most likely retain and rely on service providers for this purpose. Due to the expansion of open banking frameworks as networks, and their reliance on standardized functions which can be scaled easily,[314] it is plausible, if not probable, that a limited number of such providers will provide these services to many participants. Further, the expansion of open banking frameworks as highly connected networks, means that a service provider could quickly become critical to the open banking system's overall operation.[315] Consequently, this could result in "an ostensibly large and diverse number of entities all dependent on just a few unregulated providers for critical services, creating a substantial concentration risk and increasing the threat of contagion in the event of a service failure."[316] The sudden suspension or cessation of the services provided by one of these dominant service providers, for example because of their

311. *Id.*

312. This is another demonstration of the focus on payments and payment systems in U.K. open banking. *See supra* Part IV.C.1 and *infra* Part 5.

313. The Australian framework includes a data segregation requirement as part of its information security controls, to ensure that customer data held or stored on behalf of a data recipient is segregated from other customer data and not commingled. It offers some protection in the case of the outsourced service provider's default. *See* CDR Rules, *supra* note 213, sch. 2 r. 2.2(2)(e), at 117.

314. *See* Euro. Banking Auth., *supra* note 308.

315. *See* Zetzsche et al., *supra* note 165.

316. Wayne Byers, Austl. Prudential Regul. Auth. Chair, Peering into a Cloudy Future, Speech at Curious Thinkers Conference, Sydney (Sept. 21, 2018).

insolvency or a successful cyber-attack, would impact the ability of many participants to function in the open banking system, potentially severely impairing the communication of customer data through the system and causing a severe loss of data. Further, due to the cost and risk involved in safely storing data, it is plausible that they could be responsible for the storage of a significant proportion, or even the majority, of the customer data shared with data recipients. Consequently, the failure of just one of these highly connected providers could not only harm the communication of customer data but also significantly impact the confidence of customers and the credibility of the open banking system, causing the withdrawal of further services. As the analysis in Part I.C. above shows, this can have a systemic impact on the stability of the overall banking system. Accordingly, although the lower level of regulation of outsourcing arrangements under U.K. open banking offers greater access to customer data, the trade-off is a reduction in level of control and visibility of these arrangements compared to Australian open banking and payment systems. This makes the analysis of the legal features which preserve stability in open banking systems particularly relevant. This is conducted in the next Section of this Article.

D. *Summary*

This Section has shown that the requirements for authorization to directly participate as a data recipient are broadly comparable under open banking in Australia and the U.K. and with principles applied in banking payment systems. However, Australian open banking imposes them as a condition of access to the data sharing network whilst U.K. open banking imposes them as a condition of providing the service using data received through such a network. This conflation of the regulation of data sharing with the regulation of services provided using that data has the potential to constrain access to U.K. open banking and is inconsistent with developments in banking payment systems which seek to tailor access requirements to the risks being managed. However, the impact on participation is managed by the greater flexibility offered under U.K. open banking for indirect participation, although recent amendments to the Australian system have extended the scope of indirect participation in Australia too. Nevertheless, there remains a meaningful difference in that U.K. open banking enables data to be shared with third parties who are beyond the reach of its regulatory architecture or any other authorization relating to the holding of customer data. Also, U.K. open banking does not regulate outsourced service providers to the same extent as Australian open banking, or banking payment systems. In summary, the U.K. system has a legal design which facilitates greater access to various means of participation than either the Australian system or banking payment systems. The result of this is that the U.K. system provides less protection

with respect to the use of third parties beyond the system and with respect to outsourced service providers.

V. PRESERVING STABILITY OF PARTICIPATION IN OPEN BANKING SYSTEMS

The legal relationships between direct and indirect participants, and their service providers in an open banking system create a network of interdependencies in relation to the sharing and use of customer data. Data recipients rely on banks (and sometimes other data recipients) to share customer data so that they may provide their own services to customers and rely on agents, intermediaries, and service providers to support them in doing so. Also, data recipients and banks rely on each other to use the open banking system appropriately and to maintain its information security and stability. As explained in Part I, if a highly connected participant were to suddenly cease to provide open banking services, then not only might their customers suffer an interruption in their own business (which might provide services to others too), but also other data recipients may not be able to provide their own services. Further, the sudden withdrawal of services due to participant failure would cause customers to lose confidence in the framework, affecting still more participants, as "information contagion" spreads. Accordingly, open banking systems should incorporate legal features designed to preserve their stability beyond the requirements of authorization analyzed in Part IV above. The legal requirements relating to three key aspects of preserving stability in open banking in Australia and the U.K. include: (1) the removal of defaulting participants; (2) the protection of customer value on participant default; and (3) the impact of participant insolvency on data sharing, are comparatively analyzed below, in each case followed by evaluation against the equivalent principles in the regulation of payment systems.

A. *Removal of Defaulting Participants*

1. Comparison of Removal of Defaulting Participant in Open Banking

Under Australian open banking, the ACCC can suspend or revoke an ADR's accreditation if it is satisfied that the ADR was granted accreditation on the basis of materially false or misleading information, has been found to have contravened a law relevant to the management of customer data, or is no longer a fit and proper person to hold that level of accreditation. Accreditation can also be suspended or revoked by the ACCC if a term in a "relevant contract" where the customer is found to

be unfair,[317] is found to have breached one or more data standards or if the ACCC reasonably believes that suspension or revocation is necessary to protect consumers or to protect the security, integrity and stability of either the Register of Accredited Persons, or the information and communication technology systems that are used by CDR participants.[318] The ACCC has a further power to suspend (but not revoke) the accreditation of a data recipient if it reasonably believes that the data recipient has contravened one or more of the standards developed by the Data Standards Body, or provisions of the CCA which amounts to an offence or is a civil penalty provision, or that a relevant contract with the customer has an unfair term.[319] The ACCC can also vary the conditions on a data recipient's accreditation, including by adding new conditions.[320] This can be done without notice if notice would create a real risk of harm or abuse to an individual or adversely impact the security, integrity and stability of either the Register of Accredited Persons,[321] or the information and communication technology systems that are used by participants to disclose or collect customer data.[322]

The FCA can cancel a person's registration as an AISP if the person obtained their registration through false statements or any other irregular means, the person no longer meets the conditions for registration, the person has provided payment services other than in accordance with their authorization, the person's provision of payment services is unlawful, the person's continuation of its payment services business would constitute a threat to the stability of, or trust in, a payment system, or the cancellation is desirable to protect the interests of consumers.[323] The PSR also empowers the FCA to vary a person's registration for similar reasons, and that variation can take effect immediately, on the FCA providing notice.[324] Also, an AISP's registration in the Directory Of Open Banking Participants may be removed by the OBIE if their regulatory status is revoked.[325]

---

317. A "relevant contract" for this purpose is a "a standard form contract that is a consumer contract or a small business contract within the meaning of section 23 of the Australian Consumer Law" which arises from the good or service the consumer requested in connection with the sharing of the customer data. CDR Rules, *supra* note 213, r. 5.17(2).

318. *Id.* r. 5.17.

319. *Id.* r. 5.17 items 6, 10. *See supra* text accompanying note 317.

320. *Id.* r. 5.10.

321. This register is operated by the ACCC and includes, for each accredited person, identification details, the level of accreditation, the conditions on accreditation and whether the accreditation has been suspended or revoked. *Id.* r. 5.24.

322. *Id.* r. 5.10(3).

323. Payment Services Regulation 2017, SI 2017 No. 752, regs. 10(1), 19 (U.K.).

324. *Id.* regs. 12(1), 19.

325. Open Banking Implementation Entity, *Open Banking Guidelines for Read/Write Participants* ¶ 5.5.2 (May 2018), https://www.openbanking.org.U.K./wp-content/uploads/Guidelines-for-Read-Write-Participants.pdf [https://perma.cc/2RQR-VGPA].

Open banking in Australia and the U.K. share common elements in the rights of regulators to cancel the authorization of a defaulting ADR or AISP—each enables removal on the grounds of breaching obligations, providing false and misleading information or no longer meeting the requirements to be authorized.[326] However, there are two significant differences:

- ***Urgent suspension.*** Under each system, a process is required to be followed before a revocation or cancellation of authorisation takes effect including notification and an opportunity for the authorised person to be heard.[327] However, Australian open banking also allows accreditation to be suspended without following this process if, in the opinion of the ACCC, there are urgent grounds for the suspension and, as a result, it is not possible to comply with that process beforehand.[328] There is no equivalent under U.K. open banking, or even an ability to suspend, rather than cancel, an AISP's authorisation. This absence of an express suspension right is notable and is in contrast to the rights of the FCA with respect to some other authorisations which it grants.[329]
- ***System being protected.*** Each of Australian and U.K. open banking enables the relevant regulator to remove a participant where it is needed to protect the system's stability,[330] but the relevant system being protected in each is different. In Australian open banking, it is the Register of Accredited Persons or the "information and communication technology systems that are used by CDR participants to disclose or collect CDR data."[331] In U.K. open banking, it is "a payment system."[332] These are not the same. A threat to the stability of the information and communication technology systems used to share open banking data which would justify removal of a participant from Australian open banking would not be sufficient to remove the participant under U.K. open banking unless it also threatened the stability of a payment system.

Combined, these represent a material difference in the legal design of Australian and U.K. open banking with respect to the treatment of defaulting participants. It demonstrates again that the focus of regulation in U.K. open banking is on the payment systems which could be affected

326. CDR Rules, *supra* note 213, r. 5.17; Payment Services Regulation 2017, SI No. 752, regs. 10(1), 19 (U.K.).

327. CDR Rules, *supra* note 213, rr. 5.18, 5.19. 5.20; Payment Services Regulation 2017, SI No. 752, regs. 10(2), 10(3) (U.K.).

328. CDR Rules, *supra* note 213, r. 5.21.

329. PSR: FIN. CONDUCT AUTH., *supra* note 262, ¶ 14.11. The FCA has noted that its suspension power under the Electronic Money Regulations, 2011 (U.K.) is additional to what it possesses under the PSR: FIN. CONDUCT AUTH.

330. CDR Rules, *supra* note 213, r. 5.17(1) item 4; Payment Services Regulation 2017, SI No. 752, reg. 10(1)(g) (U.K.).

331. CDR Rules, *supra* note 213, r. 5.17.

332. Payment Services Regulation 2017, SI No. 752, reg. 10(1)(g) (U.K.).

by the use of the shared data, rather than open banking as a system itself for sharing of data.[333] In the next Section, the impact of this is evaluated against the removal of defaulting participants in payment systems.

2. Evaluation Against Removal of Defaulting Participant from Payment Systems

Due to the systemic risks which can arise in payment systems and other financial market infrastructure, it is common for there to be a right to suspend the participation of failing participants urgently if they threaten the system's stability.[334] Rights of this nature were used to impressive effect in the management of the failure of Lehman Brothers with respect to its cleared derivatives.[335] These processes involved the suspension of the Lehman entities from participation in the relevant markets and clearing systems to "prevent any further risk or positions accumulating."[336] These rights of suspension can be found in the regulations governing the primary payment systems of Australia and the U.K.,[337] and their importance can be seen in the legal obligations (with criminal penalties) imposed on all participants of these systems in Australia to inform the operator of the insolvency of any participant.[338] It is also shown in the PSR itself, which as noted above, includes threatening the stability of a payment system as a basis for the cancellation of the authorization of a payment service provider.[339]

Equivalent rights could be needed in an open banking system to remove a participant that is threatening the system's stability, or to urgently suspend a defaulting participant to avoid the accumulation of further risks. This would prevent the impact of the default of a participant (such as in relation to an information security failure) from being able to be spread to other participants through the system's connections. As noted in Part IV.A.1 above, Australian open banking includes an express

---

333. *See supra* Parts IV.A & IV.C.

334. *See* BANK FOR INT'L SETTLEMENTS, COMM. ON PAYMENT AND SETTLEMENT SYS., *supra* note 121, ¶ 7.9.8.

335. Simon Firth, *The English Law Treatment of Lehman's Derivative Positions*, *in* BANK FAILURE: LESSONS FROM LEHMAN BROTHERS, ¶ 10.04 (Dennis Faber & Niels Vermunt eds. 2017). Their resolution "occurred largely without incident—a tribute to the default processes of the exchanges and clearing houses with which the positions were held."

336. Global Ass'n of Cent. Counterparties, *Central Counterparty Default Management and the Collapse of Lehman Brothers* 2, at 2 (Apr. 2009).

337. *See* Rsrv. Bank of Austl., RITS REGULATIONS reg. 27.2 (Nov. 18, 2020); Bank of Eng., CHAPS RULES r. 6.8 (Mar. 31, 2021).

338. *Payment Systems and Netting Act 1998* (Cth.) s 7 (Austl.). The requirements in the U.K. are not imposed on all participants: Financial Markets and Insolvency (Settlement Finality) Regulations, 1999, SI No. 2979 (U.K.), reg. 22, sch. para. 5 (hereinafter Settlement Finality Regulations).

339. Payment Systems Regulation, 2017 (U.K.), reg. 10(1)(g).

right of urgent suspension of the accreditation of a data recipient comparable to those which exist in payment systems,[340] but there is no equivalent under U.K. open banking. In this context, the absence of a right to urgently suspend a participant which is endangering the U.K. system is difficult to understand. It is possible that, carefully implemented, the power to vary the conditions on an authorization under the U.K. framework could be used to achieve the same effect.[341] However, the need to do so would still lack the transparency needed to deter activities which would warrant suspension and to underpin the confidence of customers and other participants in the system.[342] Alternatively, the suspension power might not have been thought necessary in the knowledge that it would be included in the rules of the relevant payment system.[343] However, this misses the point. The suspension power under Australian open banking is intended to manage risks in the data sharing network, not risk in other networks such as those that enable payments to be made. The OBIE might be thought of as the "operator" of U.K. open banking, but it has no equivalent suspension right.[344] Accordingly, the result is that there is no transparent basis for removing a data recipient urgently even if they are threatening the data sharing framework's stability. This deprives U.K. open banking of an important means of preserving the stability of it as a communication system if a participant defaults when it is evaluated against the rights provided under banking payment systems.

B. *Protecting Customer Value on Participant Default*

1. Comparison of Protection of Customer Data in Open Banking

The primary tool for the management of default by a data recipient under Australian open banking is the ACCC's ability to suspend or revoke their accreditation, as analyzed in Part IV.A above. However, the *CDR Rules* go further by setting out detailed consequences for the treatment of shared data when these rights are exercised. They require that a person whose accreditation is surrendered, suspended or revoked:

- must not seek to collect any customer data,[345]

340. CDR Rules, *supra* note 213, r. 5.21.

341. Payment Systems Regulation, 2017 (U.K.), regs. 12(1), 19.

342. "The rules of the system should provide for clearly specified procedures for orderly withdrawal of a participant from the system, either at the participant's request, or following a decision by the system operator that the participant should withdraw." Bank for Int'l Settlements, Comm. on Payment and Settlement Sys., *supra* note 121, ¶ 3.9.2.

343. *See* Settlement Finality Regulations, *supra* note 338, sch. para 6.

344. *See generally* COMPETITION & MKTS. AUTH., RETAIL BANKING MARKET INVESTIGATION FINAL REPORT (Aug. 9, 2016).

345. CDR Rules, *supra* note 213, r. 5.23(3)(a).

- must notify each customer who has consented to their collection of data of the surrender, suspension or revocation and that, in the case of a suspension, their consents to collect and use the data may be withdrawn at any time.[346]

In the case of a suspension, the data recipient remains accredited and continues to be subject to the obligations of an accredited person.[347] In the case of a surrender or revocation, the consents to collect and use data, and the authorizations to disclose data given to the data recipient, expire.[348] Also, the data recipient must delete or de-identify the collected data in accordance with the *CDR Rules*,[349] unless they are needed for legal or dispute resolution proceedings.[350] The data recipient remains subject to the privacy safeguards relating to use and disclosure of data, including for direct marketing, of the data continue to apply.[351]

Although U.K. open banking has provisions relating to the cancellation of authorizations, there is nothing equivalent in the U.K. system which links these events to the collection, holding, and use of data. The PSR contains no provisions relating to the use of the data shared, other than in relation to the requirement for consent.[352] Further, the complexities in the interaction between PSR and GDPR arise partly because GDPR contains no provisions relating to the authorization as an AISP under PSD2. An entity's loss of authorization as an AISP will result in it no longer being able to provide the account information service and, as a result, no longer receive, use and share the data which that authorization permitted.[353] However, the U.K. system does not provide the same clarity of obligations on the data recipient, or the express protections of notification of customers and ability to withdraw consent as is provided to customers under Australian open banking. This difference should be regarded as material for two reasons. First, the customer is relying on the performance of the data recipient in relation to

346. *Id*. at r. 5.23(3)(b).

347. *Id*. at r. 5.23(2).

348. *Id*. at rr. 4.14(2), 4.26(2).

349. If an accredited person is holding customer data which they no longer need for the purpose permitted under the *CDR Rules* or the *CCA* then they are required to take the steps set out in the *CDR Rules* to destroy or de-identify that data: Competition and Consumer Act, 2010 (Cth.) s. 56EO (Austl.).

350. CDR Rules, *supra* note 213, r. 5.23(4).

351. *Id*. at r. 5.23(2). These are privacy safeguards 6, 7 and 12 contained in *Competition and Consumer Act 2010* (Cth.) ss. 56EI, 56 EJ, 56EO (Austl.).

352. For further explanation see Farrell, *supra* note 40.

353. This requires the data recipient to erase the customer's personal data "without undue delay" if, most relevantly, the data are "no longer necessary in relation to the purposes for which they were collected or otherwise processed." GDPR, *supra* note 23, art. 17.

the use and deletion of their data.[354] Accordingly, notification of the customer and enabling them to withdraw consent to further use of data is important if the capacity for the data recipient to perform its obligations is reduced. Second, the clarity of the data recipient's obligations is important if the data recipient is insolvent, as analyzed in Section C below.

2. Evaluation Against Protection of Customer Value in Payment Systems

Protection of customer value from participant default is also critical in payment systems. The historical connection between banks and payment systems and the role of banks in holding customer value as creditor and not as bailee or trustee results in some confusion in analyzing these requirements,[355] but this is clearer when considering payment system members who are not banks or clearing and settlement systems which involve the holding and delivery of obligations and property, rather than the payment of money. In these circumstances, segregation arrangements are often used to ensure the customer's assets being held by a participant for a customer are clearly identified, separately held from the assets available to the participant's creditors,[356] and able to be transferred to another participant so that the customer can continue to benefit from the system despite the participant's default.[357] These arrangements have proven instrumental in minimizing the disruption caused by the default of participants in securities and futures clearing systems,[358] as can be seen in the successes and failures of protecting customer value through segregation and portability protections in the collapse of Lehman Brothers.[359]

Neither Australian nor U.K. open banking seeks to segregate data held by a participant should it default. Neither the CCA, CDR Rules nor the PSR includes such requirements. Australian open banking includes a data

---

354. *See* Farrell, *supra* note 45.

355. *See* Awrey & van Zwieten, *supra* note 140.

356. *See* the "client money" regulations which require client funds to be segregated from a licensed entity's own assets: *Corporations Regulations 2001* (Cth.) reg. 7.8.01 (Austl.). *See also* FIN. CONDUCT AUTH., *supra* note 274, at [CASS 7.10.16].

357. *See* BANK FOR INT'L SETTLEMENTS, COMM. ON PAYMENT AND SETTLEMENT SYS. & INT'L ORG. OF SEC. COMMS, *supra* note 168, at 82. This is particularly relevant for central counterparties.

358. *See* ROY GOODE, PRINCIPLES OF CORPORATE INSOLVENCY LAW ch. 1, pts. 5, 6 (2011).

359. See the differences in the treatment of customer positions in connection with the derivative positions of Lehman Brothers entities. Lord Justice Briggs, *How Has English Law Coped With the Lehman Collapse?*, *in* BANK FAILURE: LESSONS FROM LEHMAN BROTHERS, *supra* note 335; Global Ass'n of Cent. Counterparties, *supra* note 336, at 2; Firth, *supra* note 335, ¶ 10.04; Stephen Lubben, *Lehman's Derivative Portfolio: A Chapter 11 Perspective*, *in* BANK FAILURE: LESSONS FROM LEHMAN BROTHERS, *supra* note 335; Michael J. Fleming & Asani Sarkar, *The Failure Resolution of Lehman Brothers*, 20 ECON. POL'Y REV. 177 (Dec. 2014).

segregation requirement as part of its information security controls, but this requires customer data held or stored *on behalf of a data recipient* to be segregated from other customer data and not commingled.[360] It does not require the segregation of any customer's data by the data recipient itself. Nor does either framework contain obligations for a defaulting data recipient to transfer customer data to another participant in the open banking system. However, data, unlike money, is "non-rivalrous" in that it can be used repeatedly by more than one person without reducing its functional value to its holder.[361] This means that such segregation and portability protections may not be warranted, despite the value of the data shared with the defaulting participant. The default of a data recipient does not mean that the data shared with it is lost to the customer, in the same way as customer funds received by a defaulting bank, or customer property received by a defaulting broker, could be lost. Nor is it essential that the continued sharing or use of the data by the defaulting participant be enforced, or that the data shared with the defaulting participant be repaid. Instead, the value of the data to the customer could be protected by a combination of enabling the customer to require their bank to share their data with another data recipient and requiring the defaulting data recipient deleted the customer data held by it. This enables the customer to continue to derive value from the appropriate use of their data by the performing data recipient and to prevent any loss of value to the customer from the inappropriate use of their data by the defaulting data recipient. This is consistent with the obligation to delete customer data which is imposed on a data recipient whose accreditation is revoked under the Australian system.[362] However, as noted above, there is no equivalent obligation under U.K. open banking. This is particularly relevant if the data recipient becomes insolvent.

C. *Managing Participant Insolvency*

1. Comparison of Management of Participant Insolvency in Open Banking

The laws and regulations of neither Australian nor U.K. open banking expressly contemplates the insolvency of a participant, including recipients of customer data. Under each system, a data recipient's insolvency would be a sufficient basis for the revocation (under the Australian system) and cancellation (under the U.K. system) of its authorization. As noted in Part IV.B.1 above, under Australian open

360. CDR Rules, *supra* note 213, sch. 2 r. 2.2(2)(e) (emphasis added).

361. VIKTOR MAYER-SCHÖNBERGER & KENNETH CUKIER, BIG DATA: THE ESSENTIAL GUIDE TO WORK, LIFE AND LEARNING IN THE AGE OF INSIGHT 104 (2nd ed. 2017). *See also* Martens, *supra* note 39, at 6; FLORIDI, *supra* note 113, at 90; Reimsbach-Kounatze, *supra* note 25.

362. *See* discussion *supra* Part IV.B.1.

banking, this would result in an obligation to delete or de-identify the data held by the data recipient, whilst under U.K. open banking the data recipient would have a legal obligation to no longer use the data. However, the operations of insolvency proceedings and the duties of the insolvency practitioner appointed to conduct them can complicate the performance of these obligations.

The complexity of the interaction between insolvency law and data-related obligations can be seen from two English cases. The first, *Southern Pacific Personal Loans*,[363] concerned the voluntary liquidation of a member of the Lehman Brothers group of companies and the customer data on loans granted by the company which had been redeemed. This data were not needed for the company's business, but they were needed for the company to comply with its obligations as a data controller to meet data subject access requests under the Data Protection Act 1998 (U.K.) (DPA).[364] As the cost of meeting these requests was many times the fees able to be charged for them, the liquidators sought clarification from the court that they may dispose of the data instead, and that they were not data controllers,. The court found that the liquidators were only agents of the company, including with respect to data rights and obligations, and they were not bound by the DPA as data controllers.[365] Further, the court found that as the data were "no longer required for any business of the company or for any purposes of the liquidation,"[366] the data could (and should)[367] be deleted except to the extent they were needed for data requests already made, or for the liquidation.[368] The court did not find that the liquidators could ignore the company's obligations under the DPA because "[e]nforcement action might be taken and orders might be made against the company, notwithstanding that it is in liquidation,"[369] but treated the liquidators' relationship with the data under the company's control similar to that which exists with the company's property.[370]

These principles were taken further in *Green v. SCL Group*,[371] which also concerned a subject access request given under the DPA and a

363. *Southern Pacific Personal Loans Ltd.* [2013] EWHC 2485 (U.K.).

364. *See Generally* Data Protection Act, 1998 (U.K.).

365. *Southern Pacific Personal Loans Ltd.* [2013] EWHC 2485 ¶¶ 34, 35.

366. *Id.* ¶ 39.

367. In accordance with the fifth data protection principle of the *DPA*, namely that personal data should not be kept for longer than is necessary for this purpose for which they were processed. *Id*.

368. *Id.* ¶ 40.

369. *Id.* ¶ 38.

370. The court refrained from deciding that the data was property, and instead noted that this is "a complex subject." *Id.* ¶ 34.

371. Green v. Group Ltd. & Others [2019] EWHC (Ch) 954, https://www.bailii.org/ew/cases/EWHC/Ch/2019/954.html [https://perma.cc/V8WE-TWWY].

company in the Cambridge Analytica group. Subsequent to the request being made, the company was placed into administration and the case concerned the impact of the administration on the data rights which arose in respect of that request. The court was clear that such data rights have no special status in insolvency, and the administrators were under no general duty to investigate data breaches occurring before their appointment.[372] Instead the duties of the administrators were to achieve the objectives of the administration, namely: "achieving an economic return to the creditors (not to investigating the company's compliance with data protection laws), to fulfilling their statutory duties to investigate the directors, and to exiting from the administration in an appropriate way."[373]

The court said that as insolvency is "a class remedy in which individual legal rights are transformed into rights to participate in the insolvency process, that process itself being conducted in the interests of the general body of creditors,"[374] the holder of data rights was entitled to participate in the insolvency by proving a monetary claim. Further, the court did not find that the administrators were guilty of misconduct in ignoring an enforcement notice given under the DPA as it was given to the company, and not to them, as the data controller, and it was not inappropriate for the administrators to determine that the costs of compliance with such a notice were more burdensome on creditors than non-compliance. In summary, the court was dismissive of data-related obligations having special status in insolvency and concluded that "the administration was not being run with a view to providing [the data subject] with his data."[375]

These cases show that the continued performance of statutory data-related obligations cannot be relied on in a data recipient's insolvency. This is because the insolvency practitioner conducting the insolvency proceedings "would not be held to account personally for breaches of data protection laws, where it is a regulatory requirement for a controller or other officer to be appointed and assume responsibility for the handling of that data."[376] Instead, like other obligations owed by the insolvent, they are to be converted to a monetary claim so that the creditor may participate in the sharing of the insolvent's remaining assets. There is no reason to believe that the result would be materially different under Australian insolvency law, as the relevant substantive principles are the same.[377]

372. *Id*. at 62.
373. *Id*.
374. *Id*. at 60.
375. *Id*. at 78.
376. Robert Walters, *Insolvency and Data Protection*, 42(1) BUS. L. REV. 2, 4 (2021).
377. *See* PHILIP R. WOOD, PRINCIPLES OF INTERNATIONAL INSOLVENCY (3rd ed. 2007).

However, each of these cases was based on a challenge by the insolvency practitioners to the performance of ongoing obligations with respect to the relevant data, not the data's deletion. What was missing was a clear way for the insolvency practitioners to legally rid themselves of the relevant data and the associated ongoing non-monetary obligations. In these circumstances the clear statutory obligations to delete the customer data which exist under Australian open banking could be sufficient as a basis for the insolvency practitioner to delete the relevant data. However, the absence of similar clear obligations under U.K. open banking means that the consequences of insolvency are more obscure and represent a significant difference between the systems. This is evaluated against payment systems in the next Section.

2. Evaluation Against Insolvency Law Protection for Payment Systems

Due to the importance of the functions performed by payment systems for the economy, the operation of their rules and procedures are often protected by legislation from the effect of ordinary insolvency laws.[378] These protections grant priority to payment system rules over those laws in the case of a participant's default,[379] including by permitting payments to be settled in accordance with those rules even after the insolvency of a participant has commenced.[380] These protections are an important feature in managing the stability of the payment system, the systemic risk if there is a participant default and, as a result, the confidence in the system as a whole.

Neither of the Australian nor U.K. open banking systems has any similar legal protections of the legal rights and obligations with respect to customer data in the insolvency of a data recipient. If this means that customer loses control of the use of their data in their data recipient's insolvency, and this causes confidence to be lost in open banking, then this could be of concern. However, due to an important difference between customer data and customer funds, managing this risk for open banking systems should not require the same legal protection as for payment systems. As noted in Part III.B above, customer data are non-rivalrous and, unlike customer funds, are not lost to the customer when they have been shared with a data recipient. For the customer to avoid losing value on a data recipient default, it is only necessary to compel the

---

378. *See* Banking Act 2009 (U.K.); Banking Act 1959 (Cth) (Austl.). *See also Payment Systems and Netting Act 1998* (Cth) (Austl) and Settlement Finality Regulations, *supra* note 338. *See also* GOODE, *supra* note 358, ch. 1.

379. Creating a "safe harbor" against the operation of those rules: CRANSTON, ET AL., *supra* note 142, at 355.

380. Namely, on the same day thus overriding the "zero-hour rule." *See Payment Systems and Netting Act 1998* (Cth) ss. 6, 6A (Austl); Settlement Finality Regulations, *supra* note 338, reg. 20.

data recipient to delete the customer data rather than returning the data or transferring the data to another data recipient. There isn't a need to protect the continued operation of the open banking system's rules relating to the custody and use of customer data by the data recipient if the data is deleted on the data recipient's insolvency. As noted in Part III.B, this exists in Australian open banking but not U.K. open banking. Whilst it could be expected that an insolvency practitioner would comply with this obligation, to further protect the customer, and confidence in the open banking system, it would be more aligned with the protections afforded to payment systems if it were clarified that this deletion of customer data is required even in the insolvency of the data recipient. This would enhance the confidence which customers and participants have in the open banking system.

D. *Summary*

There are clear differences in the legal design of U.K. open banking when compared to Australian open banking and banking payment systems. The ability to remove a defaulting participant from U.K. open banking is more limited than under the Australian framework or banking payment systems, as the U.K. system lacks a right to suspend a participant urgently and to remove a participant based on the threats to the data sharing system under open banking alone. Further, U.K. open banking lacks a clear obligation on a data recipient which loses its authorization to delete the customer data shared with it, unlike Australian open banking. This is particularly relevant in the circumstances of a data recipient's insolvency and represents a key difference from the protection of the customer value that is performed by customer asset segregation in banking payment systems. In summary, the U.K. system has a legal design which places less regulation on participation in the circumstances of a data recipient's default. The result of this is that the U.K. system provides fewer mechanisms to protect the stability of the open banking system or the customer data from the consequences of that default.

VI. LESSONS FOR PARTICIPATION, ACCESS AND STABILITY IN U.S. OPEN BANKING

This Article argues that if open banking is to achieve its objectives of improving competition, encouraging innovation, fostering inclusion and consumer protection then open banking's legal design needs to do more than support the functions of data portability, customer autonomy and recipient accountability. In addition, it needs to establish an effective and safe ecosystem of participation by data recipients, intermediaries and the service providers which support them. This requires a balance between the foundations of enabling access and preserving stability.

This Article demonstrates how this balance has been reached differently in two leading common law open banking systems through the legal features which enable access, by direct and indirect participation and the use of outsourcing services, and which preserve stability, by the protection of customer value on participant default and the management of participant insolvency. It has identified that the legal design of U.K. open banking compensates for more limited flexibility in access by direct participation with more flexibility in access by indirect participation, which results in a lower level of regulation of indirect participation and outsourcing relationships than under Australian open banking. It has also identified that the legal design of U.K. open banking offers less in the preservation of stability due to more limited rights to suspend participation and less clear protection of the value in customer data in participant default and insolvency.

In evaluating the differences between Australian and U.K. open banking against the equivalent requirements of banking payments systems, this Article has shown that Australian open banking is more aligned with the legal features which provide access and protect stability in those payment systems than U.K. open banking. Counter-intuitively, this is largely because U.K. open banking is established as part of the regulation of payments, whilst Australian open banking is established as the first part of a new and independent economy-wide consumer data right.

Whilst this Article's purpose is not to pass judgment on the legal design of either open banking system, as in each jurisdiction open banking has been established on the different legal foundations available and in different policy contexts, these conclusions with respect to the legal design of Australian and U.K. open banking are instructive for the decisions to be taken in the legal design of open banking in the United States. Access and stability in U.K. open banking still benefit from a broad regulatory framework which has been regarded as appropriate for the governance of data sharing between customers, banks, and data recipients. Nevertheless, the analysis has shown how discrete areas of less regulation can increase the risk to open banking as a system, in a way which would be questioned if it were to apply in banking payment systems and which could challenge the security, credibility, performance, and effectiveness of open banking systems in a similar way to that which unmanaged equivalent risks have done in banking payment systems.

This should provide three useful lessons for the legal design of open banking in the U.S. First, this analysis shows potential risks which could arise if the regulation of participation in U.S. open banking were to be materially weaker than that in either Australia or the U.K., for example if there were to be no authorization required to receive customer data. Second, this analysis demonstrates the importance of taking a systemic

approach to the legal design of open banking so that the focus is not solely on the separate relationships between consumers, banks, and data recipients. Third, this analysis shows how this systemic approach can be supported by using banking payment systems as a benchmark for evaluating, and designing, access and stability in open banking. This is an important design tool for U.S. open banking as it enables important legal features from U.S. banking payment systems to be considered in the design of U.S. open banking. By treating open banking as *a banking system for valuable data* (instead of merely providing data *on* banking) the design of the U.S. open banking system can benefit from lessons learned in enabling and protecting U.S. banking payment systems. With this analysis, open banking in the U.S. can be designed to be as effective and as safe in sharing customer data as the U.S. banking payment systems are in transferring customer funds.